

3.1

TREND MICRO™

Endpoint Encryption

Administratorhandbuch

Umfassende Endpunktverschlüsselung für gespeicherte Daten



Dokument-Nr.: APGM35732/121016

Release-Datum: Dec 2012

Geschützt durch U.S. Patent-Nr.: Zum Patent angemeldet.

In dieser Dokumentation finden Sie eine Einführung in die Hauptfunktionen des Produkts und/oder Installationsanweisungen für eine Produktionsumgebung. Lesen Sie die Dokumentation vor der Installation und Verwendung des Produkts aufmerksam durch.

Ausführliche Informationen über die Verwendung bestimmter Funktionen des Produkts sind möglicherweise in der Trend Micro Online-Hilfe und/oder der Trend Micro Knowledge Base auf der Website von Trend Micro verfügbar.

Das Trend Micro Team ist stets bemüht, die Dokumentation zu verbessern. Bei Fragen, Anmerkungen oder Anregungen zu diesem oder anderen Dokumenten von Trend Micro wenden Sie sich bitte an docs@trendmicro.com.

Bewerten Sie diese Dokumentation auf der folgenden Website:

http://www.trendmicro.com/download/documentation/rating.asp



Inhaltsverzeichnis

Vorwort

Vorwort ix
Produktdokumentation x
Dokumentationskonventionen x
Zielgruppe xi
Begriffe xii
Info über Trend Micro xiv

Kapitel 1: Trend Micro Endpoint Encryption verstehen

Info über Trend Micro Endpoint Encryption 1-2
Komponenten von Endpoint Encryption 1-2
Systemvoraussetzungen 1-5
Wichtigste Funktionen und Vorteile 1-9
Verschlüsselung verstehen 1-10
Dateiverschlüsselung 1-10
Full Disk Encryption 1-10
Schlüsselverwaltung 1-11
Info über FIPS 1-11
Verwaltung und Integration 1-12
Kontenrollen und Authentifizierung 1-13
Kontenrollen 1-13
Zugriffssteuerung nach Anwendung 1-14
Authentifizierungsoptionen nach Anwendung 1-15
Sicherheitsoptionen 1-15
Authentifizierungsmethode 1-16
Neue Funktionen in Endpoint Encryption 3.1.3 1-20
Unterstützung mehrerer Sprachen 1-20
Active Directory Synchronisierung 1-21
Verbesserungen in PolicyServer 3.1.3 1-21

Full Disk Encryption 3.1.3 - Verbesserungen 1-22

Kapitel 2: Erste Schritte mit PolicyServer

Erste Authentifizierung 2-2

Einführung in PolicyServer 2-2
PolicyServer MMC-Benutzeroberfläche 2-3

Mit Gruppen und Benutzern arbeiten 2-5
Benutzer und Gruppen definieren 2-6
Top-Gruppe hinzufügen 2-6
Neuen Benutzer zu einer Gruppe hinzufügen 2-8
Neuen Unternehmensbenutzer hinzufügen 2-10
Vorhandenen Benutzer zu einer Gruppe hinzufügen 2-12

Richtliniensteuerelemente verstehen 2-14
Optische Indikatoren für Richtlinien 2-15
Felder und Schaltflächen für Richtlinien 2-15
Richtlinien ändern 2-16

Anwendungen aktivieren 2-18

Kapitel 3: Richtlinien verstehen

Mit Richtlinien arbeiten 3-2

Richtlinienverwaltung 3-2
Richtlinie für Änderung auswählen 3-3
Richtlinien mit Bereichen bearbeiten 3-3
Richtlinien mit den Antworten "Wahr/Falsch" oder "Ja/Nein" 3-5
Richtlinien mit Mehrfach-/Einfachauswahl bearbeiten 3-7
Richtlinien mit Textzeichenfolgenargumenten bearbeiten 3-10
Richtlinien mit mehreren Optionen bearbeiten 3-11

PolicyServer Richtlinien 3-13
Richtlinien für die Admin-Konsole 3-13
Administratorrichtlinien 3-14
Authentifizierungsrichtlinien 3-15
Richtlinien für Protokollwarnungen 3-16
PDA-Richtlinien 3-16
Richtlinien für das Herunterladen von Service Packs 3-18

Richtlinien für Begrüßungsnachricht 3-18
Richtlinien für Full Disk Encryption 3-19
Allgemeine Richtlinien 3-19
PC-Richtlinien 3-21
PPC-Richtlinien 3-25
FileArmor Richtlinien 3-27
Computerrichtlinien 3-27
Verschlüsselungsrichtlinien 3-27
Anmelderichtlinien 3-30
Kennwortrichtlinien 3-31
MobileSentinel Richtlinien 3-32
Allgemeine Richtlinien 3-32
PPC-Richtlinien 3-34
KeyArmor Richtlinien 3-37
Virenschutzrichtlinien 3-37
KeyArmor Sicherheitsrichtlinien 3-38
Anmelderichtlinien 3-38
Richtlinien für Hinweismeldungen 3-40
PolicyServer Verbindungsrichtlinien 3-41
DriveArmor Richtlinien 3-41
Authentifizierungsrichtlinien 3-42
Kommunikationsrichtlinien 3-44
Geräterichtlinien 3-46
Allgemeine Richtlinien 3-47
Agent-Richtlinie 3-47
Authentifizierungsrichtlinien 3-47

Kapitel 4: Arbeiten mit Gruppen, Benutzern und Geräten

Arbeiten mit Gruppen 4-2
Top-Gruppe hinzufügen 4-2
Untergruppe hinzufügen 4-4
Gruppe ändern 4-5
Gruppe entfernen 4-5
Arbeiten mit Offline-Gruppen 4-5
Offline-Gruppe erstellen 4-6

Offline-Gruppe aktualisieren 4-9

Arbeiten mit Benutzern 4-10
Benutzer zu PolicyServer hinzufügen 4-10
Benutzer suchen 4-14
Benutzer ändern 4-15
Gruppenmitgliedschaft eines Benutzers anzeigen 4-15
Neuen Benutzer zu einer Gruppe hinzufügen 4-16
Vorhandenen Benutzer zu einer Gruppe hinzufügen 4-18
Standardgruppe eines Benutzers ändern 4-20
Benutzer das Installieren in eine Gruppe erlauben 4-21
Einzelne Benutzer aus einer Gruppe entfernen 4-22
Alle Benutzer aus einer Gruppe entfernen 4-22
Gelöschtes Benutzer wiederherstellen 4-23
Arbeiten mit Kennwörtern 4-24

Arbeiten mit Geräten 4-32
Gerät zu einer Gruppe hinzufügen 4-32
Gerät aus einer Gruppe entfernen 4-34
Gerät aus dem Unternehmen entfernen 4-35
Verzeichnisinhalte anzeigen 4-36
Geräteattribute anzeigen 4-36
Verzeichnisüberwachung anzeigen 4-37
Gerät auslöschen 4-38
Gerät sperren 4-38
Gerät neu starten 4-39
Gelöschtes Gerät wiederherstellen 4-39

Kapitel 5: Mit Full Disk Encryption arbeiten

Endpoint Encryption Tools 5-2

Full Disk Encryption Preboot Authentifizierung 5-2
Menüoptionen 5-3
Netzwerkverbindung 5-4
Bildschirmtastatur 5-4
Tastaturbelegung ändern 5-5
Authentifizierungsmethode ändern 5-5
Kennwörter ändern 5-6
Remote-Hilfe 5-9

SmartCard 5-11
Selbsthilfe 5-13
Full Disk Encryption Konnektivität 5-15
Aktualisieren von Full Disk Encryption Clients 5-16
Full Disk Encryption – Wiederherstellungskonsole 5-16
Auf die Wiederherstellungskonsole zugreifen 5-18
Auf die Wiederherstellungskonsole von Windows aus zugreifen . 5-18
"Festplatte entschlüsseln" verwenden 5-19
Partitionen bereitstellen 5-21
Bootsektor wiederherstellen 5-21
Full Disk Encryption Benutzer verwalten 5-22
Richtlinien verwalten 5-24
Protokolle anzeigen 5-25
Netzwerk-Setup 5-25
Full Disk Encryption Wiederherstellungsmethoden 5-27
Reparatur-CD 5-29
Daten mit der Reparatur-CD wiederherstellen 5-31

Kapitel 6: Mit FileArmor arbeiten

FileArmor Authentifizierung 6-2
Erste Authentifizierung bei FileArmor 6-2
FileArmor Domänenauthentifizierung 6-3
FileArmor Smartcard-Authentifizierung 6-4
FileArmor ColorCode-Authentifizierung 6-5
FileArmor PIN-Authentifizierung 6-5
Kennwortänderung in FileArmor 6-6
Erzwungene Kennwortzurücksetzung 6-6
FileArmor Task-Leistensymbolmenü 6-8
Mit PolicyServer synchronisieren 6-10
Offline-Dateien mit PolicyServer synchronisieren 6-10
PolicyServer wechseln 6-11
FileArmor Verschlüsselung 6-11
FileArmor Verschlüsselung mit lokalem Schlüssel 6-12
FileArmor Verschlüsselung mit gemeinsamem Schlüssel 6-13
FileArmor Verschlüsselung mit festem Kennwort 6-14

Verschlüsselung digitaler Zertifikate mit FileArmor 6-15
FileArmor – Archivieren und brennen 6-16
Archiv mit einem festen Kennwort brennen 6-16
Archiv mit einem Zertifikat brennen 6-16
FileArmor Sicheres Löschen 6-17

Kapitel 7: Mit KeyArmor arbeiten

KeyArmor Authentifizierung 7-2
Erste Authentifizierung bei KeyArmor 7-2
Authentifizierungsmethode ändern 7-3
Festes Kennwort 7-3
KeyArmor Funktionen 7-4
Gerätekomponenten 7-4
Dateien mit KeyArmor schützen 7-5
Keine Informationen hinterlassen 7-5
KeyArmor Antivirus-Updates und -aktivitäten 7-5
KeyArmor Benachrichtigung zur Festplattenüberprüfung 7-6
KeyArmor verwenden 7-6
Warnung zu unverschlüsselten Geräten 7-6
KeyArmor Taskleiste 7-7
KeyArmor Menü 7-8
Dateien mit KeyArmor schützen 7-13
KeyArmor Aktivitätsprotokollierung 7-14
KeyArmor sicher entfernen 7-14
Vollständige Suche von KeyArmor 7-15
Ein KeyArmor Gerät einem anderen Benutzer neu zuweisen 7-17
Ein gelöschtes KeyArmor Gerät wieder zum Unternehmen hinzufügen 7-18

Kapitel 8: Arbeiten mit Protokollen und Berichten

Protokollereignisse 8-2
Protokollereignisse verwalten 8-2
Warnungen 8-3
PolicyServer Warnungen einrichten 8-3

PolicyServer zur Weiterleitung von SMS und E-Mail-Versand aktivieren 8-4

Berichte 8-6
Berichtoptionen 8-6
Berichtssymbole 8-7
Berichttypen 8-7
Anzeigen von Berichten 8-10
Zeitgesteuerte Berichte 8-11
Anzeigen von Berichtsfehlern 8-11

Kapitel 9: Unterstützung erhalten

Trend Community 9-2

Support-Portal 9-2

Kontaktaufnahme mit dem technischen Support 9-3
Probleme schneller lösen 9-3

TrendLabs 9-4

Anhang A: PolicyServer Nachrichten-IDs

Stichwortverzeichnis

Stichwortverzeichnis IN-1



Vorwort

Vorwort

Willkommen beim Administratorhandbuch für Trend Micro™ Endpoint Encryption. Dieses Handbuch erläutert die wichtigsten Aspekte von Endpoint Encryption: Sicherheitsarchitektur, Verschlüsselung, Authentifizierung und Endpunkt-Verwaltung. Die Themen umfassen die Verwendung von Server- und Endpunkt-Clientanwendungen zur Unterstützung von Sicherheitszielen, die Bereitstellung von Benutzern, Gruppen und Geräten zum Implementieren von Richtlinien und die Verwendung von Berichten und Protokollen zum Analysieren von Unternehmenssicherheit. Diese Anleitung enthält ebenfalls Informationen zur Fehlerbehebung von Konfigurationen, zur Verwendung von Tools und zum Beheben von Problemen.

Das Vorwort umfasst folgende Themen:

- *Produktdokumentation auf Seite x*
- *Dokumentationskonventionen auf Seite x*
- *Zielgruppe auf Seite xi*
- *Begriffe auf Seite xii*
- *Info über Trend Micro auf Seite xiv*

Produktdokumentation

In der Dokumentation zu Trend Micro Endpoint Encryption sind folgende Dokumente enthalten:

TABELLE 1. Produktdokumentation

DOKUMENT	BESCHREIBUNG
Installationshandbuch	Im Installationshandbuch werden die Systemvoraussetzungen beschrieben. Es enthält zudem detaillierte Anweisungen zur Einrichtung, Installation und Migration sowie zum Upgrade von PolicyServer und den Endpunkt-Clients.
Administratorhandbuch	Im Administratorhandbuch werden die Produktkonzepte und -funktionen erläutert. Außerdem enthält es ausführliche Informationen zur Konfiguration und Verwaltung von PolicyServer und den Endpunkt-Clients.
Readme-Datei	Die Readme-Datei enthält aktuelle Produktinformationen, die in der Online-Hilfe oder im Benutzerhandbuch noch nicht erwähnt sind. Zu den Themen gehören die Beschreibung neuer Funktionen, Lösungen bekannter Probleme und eine Liste bereits veröffentlichter Produktversionen.
Knowledge Base	Eine Online-Datenbank mit Informationen zur Problemlösung und Fehlerbehebung. Sie enthält aktuelle Hinweise zu bekannten Softwareproblemen. Die Knowledge Base finden Sie im Internet unter folgender Adresse: http://esupport.trendmicro.com



Hinweis

Die Dokumentation steht unter folgender Adresse zum Download bereit:

http://docs.trendmicro.com/de-de/home.aspx

Dokumentationskonventionen

In der Dokumentation werden die folgenden Konventionen verwendet:

TABELLE 2. Dokumentationskonventionen

KONVENTION	BESCHREIBUNG
GROSSSCHREIBUNG	Akronyme, Abkürzungen und die Namen bestimmter Befehle sowie Tasten auf der Tastatur
Fettdruck	Menüs und Menübefehle, Schaltflächen, Registerkarten und Optionen
Kursivdruck	Referenzen auf andere Dokumente
`Schreibmaschinenschrift`	Beispiele für Befehlszeilen, Programmcode, Internet-Adressen, Dateinamen und Programmanzeigen
Navigation > **Pfad**	Navigationspfad für den Zugriff auf ein bestimmtes Fenster Beispiel: **Datei** > **Speichern** bedeutet, auf der Benutzeroberfläche auf **Datei** und dann auf **Speichern** zu klicken
Hinweis	Konfigurationshinweise
Tipp	Empfehlungen oder Vorschläge
Wichtig	Informationen zu erforderlichen oder standardmäßigen Konfigurationseinstellungen und Produkteinschränkungen
Warnung!	Kritische Aktionen und Konfigurationsoptionen

Zielgruppe

Dieses Handbuch wurde für IT-Administratoren geschrieben, die Trend Micro Endpoint Encryption in mittleren bis großen Unternehmen einsetzen. Es richtet sich zudem an Helpdesk-Mitarbeiter, die Benutzer, Gruppen, Richtlinien und Geräte

verwalten. In dieser Dokumentation werden grundlegende Kenntnisse zu Geräten, Netzwerken und Sicherheit vorausgesetzt. Dazu gehören:

- Setup und Konfiguration der Geräte-Hardware
- Partitionierung, Formatierung und Wartung der Festplatte
- Client-Server-Architektur

Begriffe

Die folgende Tabelle enthält die Terminologie, die innerhalb der Dokumentation verwendet wird:

TABELLE 3. Endpoint Encryption Terminologie

BEGRIFF	BESCHREIBUNG
Authentifizierung	Der Prozess des Identifizierens eines Benutzers.
ColorCode™	Ein Kennwort mit einer Farbfolge.
Command Line Helper	Mit dem Command Line Helper können verschlüsselte Werte erzeugt werden, die als sichere Anmeldedaten beim Erstellen von Installationsskripts verwendet werden können.
Command Line Installer Helper	Mit dem Command Line Installer Helper können verschlüsselte Werte erzeugt werden, die als sichere Anmeldedaten beim Erstellen von Skripts für automatisierte Installationen verwendet werden können.
Gerät	Computer, Laptop oder Wechselmedium (externes Laufwerk, USB-Laufwerk).
Domänenauthentifizierung	SSO (Single-Sign-On) mit Hilfe von Active Directory.
DriveTrust™	Hardware-basierte Verschlüsselungstechnologie von Seagate™.
Endpunkt-Client	Ein Gerät, auf dem eine Endpoint Encryption Anwendung installiert ist.

Begriff	Beschreibung
FileArmor	Der Endpoint Encryption Client für die Verschlüsselung von Dateien und Ordnern auf lokalen Laufwerken und Wechselmedien.
FIPS	Federal Information Processing Standard. Der Datenverarbeitungsstandard der US-Regierung.
Festes Kennwort	Ein Standardbenutzerkennwort, das aus Buchstaben und/ oder Ziffern und/oder Sonderzeichen besteht.
Full Disk Encryption	Der Endpoint Encryption Client für die Verschlüsselung von Hardware und Software mit Preboot-Authentifizierung.
KeyArmor	Der Endpoint Encryption Client für ein durch ein Kennwort geschütztes verschlüsseltes USB-Laufwerk.
OCSP	Das OCSP (Online Certificate Status Protocol) ist ein für digitale X.509-Zertifikate verwendetes Internet-Protokoll.
OPAL	Die Subsystemklasse für Sicherheit der Trusted Computing Group für Client-Geräte.
Kennwort	Alle Arten von Authentifizierungsdaten, wie beispielsweise ein festes Kennwort, eine PIN und ein ColorCode.
PolicyServer	Der zentrale Verwaltungsserver, der die Verschlüsselungs- und Authentifizierungsrichtlinien an Endpunkt-Clients bereitstellt (Full Disk Encryption, FileArmor, KeyArmor).
SED	Secure Encrypted Device (sicher verschlüsseltes Gerät). Eine Festplatte oder ein anderes Gerät, das verschlüsselt wurde.
Smartcard	Eine physische Karte wird in Verbindung mit einer PIN oder einem festen Kennwort verwendet.
PIN	Eine persönliche Identifikationsnummer, die im Allgemeinen für Automatentransaktionen verwendet wird.
Wiederherstellungskonsole	Wiederherstellung eines Geräts beim Ausfall des primären Betriebssystems, beim Beheben von Netzwerkproblemen und beim Verwalten von Benutzern, Richtlinien und Protokollen.

BEGRIFF	BESCHREIBUNG
Remote-Hilfe	Interaktive Authentifizierung für Benutzer, die ihre Anmeldedaten vergessen haben, oder für Geräte, deren Richtlinien nicht innerhalb eines bestimmten Zeitraums synchronisiert wurden.
Reparatur-CD	Verwenden Sie diese startfähige CD, um das Laufwerk zu entschlüsseln, bevor Sie Full Disk Encryption im Falle einer Beschädigung der Festplatte entfernen.
RSA SecurID	Ein Mechanismus zum Ausführen der Zwei-Faktor-Authentifizierung für einen Benutzer bei einer Netzwerkressource.
Selbsthilfe	Kombinationen aus Fragen und Antworten, mit denen ein Benutzer ein vergessenes Kennwort zurücksetzen kann, ohne sich an den Support zu wenden.

Info über Trend Micro

Trend Micro, weltweit führend in der Internet-Content-Security und der Bewältigung von Bedrohungen, hat sich als Ziel gesetzt, den globalen Austausch von digitalen Informationen für Unternehmen und Endverbraucher sicher zu machen. Mit einer Erfahrung von über 20 Jahren bietet Trend Micro Client-, Server- und Cloud-basierte Lösungen, die neue Bedrohungen schneller unterbinden und die Daten in physischen, virtuellen und Cloud-Umgebungen schützen.

Da neue Bedrohungen und Schwachstellen immer wieder auftauchen, bleibt Trend Micro seiner Verpflichtung treu, seine Kunden beim Sichern von Daten, Einhalten der Konformität, Senken der Kosten und Wahren der Geschäftsintegrität zu unterstützen. Weitere Informationen finden Sie unter:

http://www.trendmicro.com

Trend Micro und das Trend Micro T-Ball-Logo sind Marken von Trend Micro Incorporated und in einigen Rechtsgebieten eingetragen. Alle anderen Marken- und Produktnamen sind Marken oder eingetragene Marken der entsprechenden Unternehmen.



Kapitel 1

Trend Micro Endpoint Encryption verstehen

Trend Micro™Endpoint Encryption bietet stabilen Datenschutz und Gerätesteuerung für viele verschiedene Geräte und Medien, einschließlich Laptops, Desktops, Tablets, CDs, DVDs, USB-Laufwerke und andere Wechselmedien.

Dieses Kapitel umfasst folgende Themen:

- *Info über Trend Micro Endpoint Encryption auf Seite 1-2*
- *Wichtigste Funktionen und Vorteile auf Seite 1-9*
- *Verschlüsselung verstehen auf Seite 1-10*
- *Systemvoraussetzungen auf Seite 1-5*
- *Kontenrollen und Authentifizierung auf Seite 1-13*
- *Neue Funktionen in Endpoint Encryption 3.1.3 auf Seite 1-20*

Info über Trend Micro Endpoint Encryption

Trend Micro Endpoint Encryption ist eine vollständig integrierte Hardware- und Software-basierte Verschlüsselungslösung zum Schutz für Laptops, Desktops, Dateien und Ordner, Wechselmedien und verschlüsselte ESB-Laufwerke mit eingebautem Antivirus-/Anti-Malware-Schutz. Mit Endpoint Encryption können Administratoren mit einer einzigen Management-Konsole flexibel eine Kombination aus Hardware- und Software-basierter Verschlüsselung mit voller Transparenz für Endbenutzer verwalten.

Trend Micro Endpoint Encryption stellt einen durchgängigen Datenschutz durch die Verschlüsselung gemäß FIPS 140-2 für folgende Daten bereit: Daten, die sich auf dem Verwaltungsserver befinden, alle Daten, die zum oder vom Server übertragen werden, alle Daten, die auf dem Endpunkt-Gerät gespeichert werden, sowie alle lokal gespeicherten Client-Protokolle.

Mit zertifizierter FIPS 140-2-Kryptographie bietet Endpoint Encryption die folgenden Vorteile:

- Umfassender Datenschutz durch vollständig integrierte Full Disk Encryption sowie durch Verschlüsselung von Dateien, Ordnern, USB-Laufwerken und Wechselmedien.
- Zentrale Richtlinienverwaltung und Schlüsselverwaltung über einen einzelnen Verwaltungsserver und eine einzelne Management-Konsole.
- Geräteverwaltung durch Sammeln von gerätespezifischen Informationen, Gerätesperre und Wiederherstellung sowie anhand der Möglichkeit zum Löschen aller Endpunktdaten.
- Erweiterte Berichtsfunktion und erweitertes Auditing in Echtzeit zur Einhaltung der Sicherheitsrichtlinien.

Komponenten von Endpoint Encryption

Endpoint Encryption besteht aus einem zentralen Verwaltungsserver (PolicyServer Web-Service), der die Richtlinien- und Protokolldatenbanken (MobileArmor DB), die LDAP-Authentifizierung mit Active Directory und alle Client-Server-Aktivitäten verwaltet. Endpoint Encryption Clients verfügen über keine direkte Schnittstelle zu PolicyServer und müssen die Verbindung über den Client-Web-Service herstellen. Eine

Darstellung dieser Architektur finden Sie unter *Abbildung 1-1: Endpoint Encryption Client-Server-Architektur auf Seite 1-3*.



Hinweis

Die Porteinstellungen für den gesamten HTTP-Datenverkehr können zum Zeitpunkt der Installation oder über Einstellungen auf dem Endpoint Encryption Client konfiguriert werden.

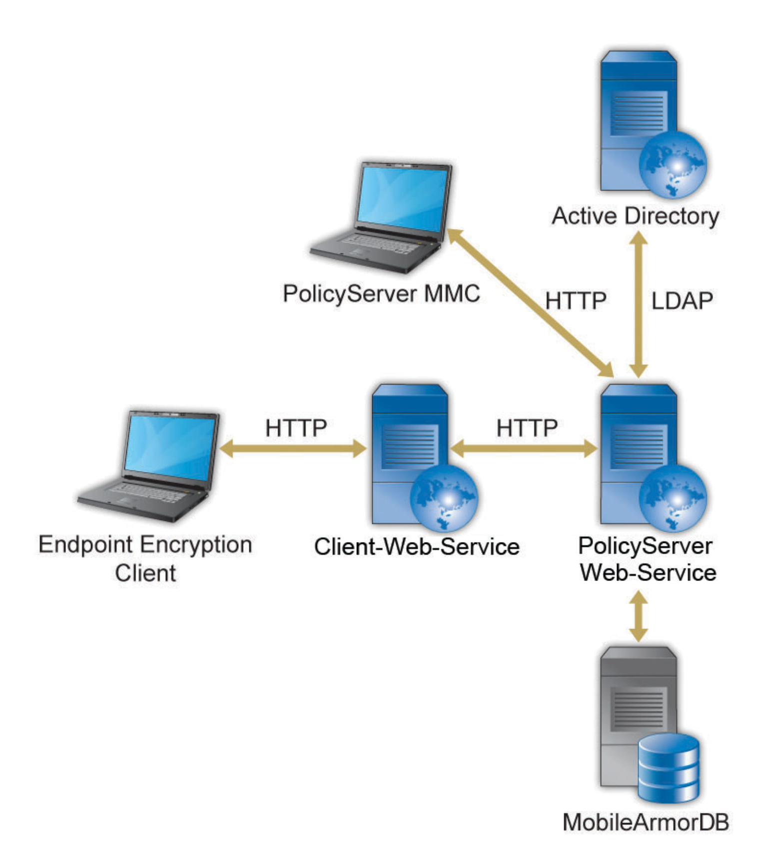


ABBILDUNG 1-1. Endpoint Encryption Client-Server-Architektur

In der folgenden Tabelle werden diese Komponenten beschrieben.

TABELLE 1-1. Komponenten von Endpoint Encryption

KOMPONENTE	BESCHREIBUNG
PolicyServer Web-Service	Der IIS-Web-Service für die zentrale Verwaltung der Administration, Authentifizierung und Berichterstellung im Zusammenhang mit Richtlinien.
PolicyServer MMC	Die PolicyServer Microsoft™ Management-Konsole (MMC) ist die Oberfläche zur Steuerung von PolicyServer.
Endpoint Encryption client	Ein Endpoint Encryption Client ist jedes Gerät, auf dem entweder Full Disk Encryption, FileArmor oder KeyArmor installiert ist. • Full Disk Encryption bietet Hardware- und Software-basierte Full Disk Encryption sowie Preboot-Authentifizierung. • FileArmor bietet Datei- und Ordnerverschlüsselung für Inhalte auf lokalen Festplatten und Wechselmedien. • KeyArmor ist ein robustes, verschlüsseltes USB-Laufwerk mit integriertem Virenschutz.
MobileArmorDB	Die Microsoft™ SQL Server Datenbank, in der alle Details zu Benutzern, Richtlinien und Protokollen gespeichert werden.
Active Directory	Der PolicyServer Web-Service synchronisiert Benutzerkontoinformationen durch Kommunikation mit Active Directory über LDAP. Die Kontoinformationen werden lokal in der MobileArmorDB zwischengespeichert. **Hinweis** Active Directory ist optional.
Client-Web-Service	Der IIS-Web-Service, den Endpoint Encryption Clients für die Kommunikation mit dem PolicyServer Web-Service verwenden.

Systemvoraussetzungen

Die unten stehenden Tabellen geben einen Überblick über die Systemvoraussetzungen für Endpoint Encryption.

TABELLE 1-2. Hardware-Voraussetzungen für PolicyServer

SEPARATE HOSTS		EINZELNER HOST
PolicyServer Host (3.000 Benutzer)	SQL-Server-Host (3.000 Benutzer)	PolicyServer und SQL-Server (1.500 Benutzer)
• 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Prozessoren • 4GB RAM • 40 GB Festplattenspeicher	• 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Prozessoren • 8GB RAM • 100GB Festplattenspeicher	• 2 GHz Quad Core Core2 Intel™ Xeon™ Prozessoren • 8GB RAM • 120GB Festplattenspeicher

TABELLE 1-3. Software-Mindestvoraussetzungen für PolicyServer

FUNKTION	VORAUSSETZUNG
Betriebssystem	• Windows Server 2003 SP2 32/64 Bit • Windows Server 2008 oder 2008 R2 64 Bit
Anwendungen und Einstellungen	• Anwendungsserver • IIS • ASP (Active Server Pages) zulassen • ASP.NET zulassen • .Net Framework 2.0 SP2 **Hinweis** PolicyServer 3.1.3 benötigt zwei IIS-Standorte. Die PolicyServer-Verwaltungsschnittstelle und die Client-Anwendungsschnittstelle müssen an verschiedenen IIS-Speicherorten installiert werden.

Funktion	Voraussetzung
Datenbank	• Microsoft SQL 2005/2008/2008 R2 • Microsoft SQL Express 2005(SP3)/2008 • Mixed Mode Authentication (SA-Kennwort) installiert • Berichtsdienste installiert

Tabelle 1-4. Full Disk Encryption Systemvoraussetzungen

Vorgang	Voraussetzung
Prozessor	Intel™ Core™ 2 oder kompatibler Prozessor.
Arbeitsspeicher	• Mindestens: 1GB
Festplattenspeicher	• Mindestens: 30GB • Erforderlich: 20% verfügbaren Festplattenspeicher • Erforderlich: 256 MB zusammenhängender freier Speicher
Netzwerkverbindung	Kommunikation mit PolicyServer 3.1.3 für verwaltete Installationen erforderlich
Betriebssysteme	• Windows 8™ (32/64 Bit) • Windows 7™ (32/64 Bit) • Windows Vista™ mit SP1 (32/64 Bit) • Windows XP™ mit SP3 (32 Bit)

VORGANG	VORAUSSETZUNG
Andere Software	Weitere Voraussetzungen für Windows 8: • Microsoft .NET Framework 3.5 ist aktiviert • Anweisungen zum Ändern der Startreihenfolge für Geräte mit UEFI finden Sie im Installationshandbuch für Endpoint Encryption. Weitere Voraussetzungen für Clients unter Windows XP: • Microsoft .NET Framework 2.0 SP1 oder höher • Microsoft Windows Installer 3.1
Festplatte	• Seagate DriveTrust-Laufwerke • Seagate OPAL- und OPAL 2-Laufwerke **Hinweis** • RAID- und SCSI-Festplatten werden nicht unterstützt. • Full Disk Encryption für Windows 8 unterstützt keine RAID-, SCSI-, eDrive- oder OPAL 2-Laufwerke.
Andere Hardware	ATA-, AHCI- oder IRRT-Festplattencontroller

TABELLE 1-5. Systemvoraussetzungen für FileArmor

VORGANG	VORAUSSETZUNG
Prozessor	Intel™ Core™ 2 oder kompatibler Prozessor.
Arbeitsspeicher	• Mindestens: 512MB • Empfohlen: 1GB
Festplattenspeicher	• Mindestens: 2GB • Erforderlich: 20% verfügbaren Festplattenspeicher
Netzwerkverbindung	Kommunikation mit PolicyServer für verwaltete Installationen erforderlich

VORGANG	VORAUSSETZUNG
Betriebssysteme	• Windows 8™ (32/64 Bit) • Windows 7™ (32/64 Bit) • Windows Vista™ mit SP1 (32/64 Bit) • Windows XP™ mit SP3 (32 Bit)
Andere Software	Weitere Voraussetzungen für Windows 8: • Microsoft .NET Framework 3.5 ist aktiviert • Anweisungen zum Ändern der Startreihenfolge für Geräte mit UEFI finden Sie im Installationshandbuch für Endpoint Encryption. Weitere Voraussetzungen für Clients unter Windows XP: • Microsoft .NET Framework 2.0 SP1 oder höher • Microsoft Windows Installer 3.1

TABELLE 1-6. Systemvoraussetzungen für KeyArmor

VORGANG	VORAUSSETZUNG
Hardware	USB-2.0-Port
Netzwerkverbindung	Kommunikation mit PolicyServer für verwaltete Installationen erforderlich
Betriebssysteme	• Windows 7™ (32/64 Bit) • Windows Vista™ mit SP1 (32/64 Bit) • Windows XP™ mit SP3 (32 Bit)
Andere Software	Weitere erforderliche Software bei der Installation auf Windows XP™: • Microsoft .NET Framework 2.0 SP1 oder höher

Wichtigste Funktionen und Vorteile

Endpoint Encryption umfasst die folgenden Funktionen und bietet die folgenden Vorteile:

TABELLE 1-7. Wichtigste Funktionen in Endpoint Encryption

FUNKTION	VORTEILE
Verschlüsselung	• Schutz durch Full Disk Encryption, einschließlich MBR (Master Boot Record), Betriebssystem und alle Systemdateien. • Hardware- und Software-basierte Verschlüsselung für gemischte Umgebungen.
Authentifizierung	• Flexible Authentifizierungsmethoden, einschließlich Einzel- und Multi-Faktor-Authentifizierung. • Richtlinienaktualisierungen vor der Authentifizierung und dem Systemstart. • Konfigurierbare Aktionen für den Schwellenwert für die Eingabe falscher Kennwörter.
Geräteverwaltung	• Richtlinien zum Schutz von Daten auf PCs, Laptops, Tablets, USB-Laufwerken, CDs und DVDs. • Möglichkeit zum Sperren, Löschen oder Auslöschen eines Geräts.
Zentrale Verwaltung	• Vollzugriff auf Verschlüsselung, Überwachung und Datenschutz. • Automatisierte Durchsetzung von Richtlinien mit Korrekturen an Sicherheitsereignissen.
Aufzeichnung von Protokollen, Berichten und Auditing	• Analysieren von Nutzungsstatistik mit geplanten Berichten und Warnmeldungen.

Verschlüsselung verstehen

Verschlüsselung bezeichnet den Vorgang, mit dem Daten unlesbar gemacht werden, wenn kein Zugriff auf den zur Verschlüsselung verwendeten Schlüssel besteht. Die Verschlüsselung kann durch eine Software- oder Hardware-basierte Verschlüsselung (oder eine Kombination aus beidem) vorgenommen werden, um sicherzustellen, dass Daten lokal auf einem Gerät, auf einem Wechselmedium, in bestimmten Dateien und Ordnern und beim Durchqueren von Netzwerken oder des Internets geschützt werden. Die Endpunktverschlüsselung ist das wichtigste Mittel, um die Datensicherheit zu gewährleisten und die Einhaltung gesetzlicher Vorschriften zum Datenschutz sicherzustellen.

Dateiverschlüsselung

FileArmor schützt einzelne Dateien und Ordner auf lokalen Festplatten und auf Wechselmedien (USB-Laufwerken). Administratoren können Richtlinien festlegen, die angeben, welche Ordner und Laufwerke auf dem Gerät verschlüsselt sind, und die Richtlinien zu verschlüsselten Daten auf Wechselmedien festlegen. Die Datei- und Ordnerverschlüsselung wird durchgeführt, nachdem die Authentifizierung stattgefunden hat.

FileArmor kann auch verschiedene Dateien mit unterschiedlichen Schlüsseln schützen, was Administratoren ermöglicht, Zugriffsrichtlinien für ein Gerät und separate Richtlinien für den Zugriff auf bestimmte Dateien festzulegen. Dies ist in Umgebungen nützlich, in denen mehrere Benutzer auf einen Endpunkt zugreifen.

Full Disk Encryption

Full Disk Encryption ist die häufigste Verschlüsselungslösung, die heute auf Endpunkten eingesetzt wird, weil Sie alle Laufwerksdaten inkl. dem Betriebssystem, Programmdateien, temporäre Dateien und Endbenutzerdateien sichert. Viele Full Disk Encryption Anwendungen erhöhen zudem die Betriebssystemsicherheit, indem sie den Benutzer dazu auffordern, sich vor dem Starten bzw. Entsperren des Laufwerks und vor dem Zugriff auf das Betriebssystem zu authentifizieren.

Als eine Verschlüsselungslösung bietet Trend Micro Full Disk Encryption sowohl Software-basierte als auch Hardware-basierte Verschlüsselung. Während Hardware-

basierte Verschlüsselung leichter auf neuer Hardware bereitgestellt und verwaltet werden kann und eine höhere Leistungsstufe bietet, ist für die Software-basierte Verschlüsselung keine Hardware erforderlich und die Bereitstellung auf vorhandenen Endpunkten ist billiger. Trend Micro PolicyServer kann Full Disk Encryption zentral verwalten und bietet Unternehmen die Flexibilität, Software-basierte oder Hardware-basierte verschlüsselte Geräte nach Bedarf einzusetzen.

Einzigartig an Endpoint Encryption ist eine netzwerkorientierte Funktion, die Richtlinien in Echtzeit aktualisiert, bevor die Authentifizierung zugelassen wird. Endpoint Encryption ermöglicht Administratoren, ein Laufwerk zu sperren oder per Wipe zu löschen, bevor auf das Betriebssystem (und auf vertrauliche Daten) zugegriffen werden kann.

Schlüsselverwaltung

Nicht verwaltete Verschlüsselungsprodukte erfordern, dass Administratoren oder Benutzer den Verschlüsselungsschlüssel auf einem USB-Gerät aufbewahren. Endpoint Encryption sichert und hinterlegt Verschlüsselungsschlüssel transparent, während es einem Administrator ermöglicht, sich mit einem Administratorschlüssel bei dem geschützten Gerät anzumelden, um geschützte Daten wiederherzustellen.

KeyArmor USB-Geräte schützen Daten mit ständig verfügbarer Hardware-Verschlüsselung und integriertem Antivirus-/Anti-Malware-Schutz, um strenge gesetzliche Vorschriften und Richtlinien zu erfüllen. Mit KeyArmor haben Administratoren vollständige Transparenz und Kontrolle darüber, wer USB-Geräte zu welchem Zeitpunkt, an welchem Ort im Unternehmen und auf welche Weise einsetzt.

Info über FIPS

Die *Federal Information Processing Standard (FIPS) Publication 140-2* ist ein Gerätesicherheitsstandard der US-amerikanischen Regierung, der die Sicherheitsstandards für Verschlüsselungsmodule vorgibt. FIPS 140-2 beinhaltet vier Sicherheitsstufen:

TABELLE 1-8. FIPS 140-2-Sicherheitsstufen

STUFE	BESCHREIBUNG
Stufe 1	Alle Verschlüsselungskomponenten müssen sich auf der Produktionsstufe befinden und dürfen keine Sicherheitslücken aufweisen.
Stufe 2	Beinhaltet alle Anforderungen von Stufe 1 und fügt physischen Manipulationsbeweis und rollenbasierte Authentifizierung hinzu.
Stufe 3	Beinhaltet alle Anforderungen von Stufe 2 und fügt physischen Manipulationswiderstand und identitätsbasierte Authentifizierung hinzu.
Stufe 4	Beinhaltet alle Anforderungen von Stufe 3 und fügt weitere physische Sicherheitsanforderungen hinzu.

Endpoint Encryption stellt einen durchgängigen Datenschutz durch die Verschlüsselung gemäß FIPS 140-2 für Daten auf dem Policy Server bereit: alle Daten, die zwischen dem PolicyServer und Endpunkt-Clients übertragen werden, alle Daten, die auf dem Endpunkt-Gerät gespeichert werden sowie alle lokal gespeicherten Client-Protokolle.

Verwaltung und Integration

Wenn Endbenutzer einen verstärkten Datenschutz auf verschiedenen Gerätetypen benötigen, von denen die meisten unterschiedliche Verschlüsselungstypen erfordern, senkt eine zentral verwaltete und integrierte Endpunktverschlüsselungslösung die Verwaltungs- und Wartungskosten. Endpoint Encryption ist eine zentral verwaltete Lösung, die folgende Datenschutzfunktionen ermöglicht:

- Zentrales und transparentes Aktualisieren der Endpunktverschlüsselungs-Clients, wenn neue Versionen veröffentlicht werden
- Verwalten und Nutzen von Sicherheitsrichtlinien für Einzelpersonen und Gruppen von einem einzigen Richtlinienserver aus
- Steuern der Kennwortstärke und Regelmäßigkeit von Kennwortänderungen
- Aktualisieren von Sicherheitsrichtlinien in Echtzeit vor der Authentifizierung, um Benutzer-Anmeldedaten vor dem Booten des Betriebssystems zu widerrufen

Kontenrollen und Authentifizierung

Trend Micro Endpoint Encryption bietet Administratoren verschiedene Kontenrollen und Authentifizierungsmethoden für die jeweiligen Anforderungen, einschließlich Multifaktor-Authentifizierung.

Kontenrollen

Endpoint Encryption umfasst mehrere unterschiedliche Kontentypen, die für unterschiedlichen Rollen in einem Unternehmen gedacht sind. Diese Rollen bestimmen, wie Konten auf verschiedene Aufgaben zugreifen und sie ausführen.

TABELLE 1-9. Endpoint Encryption Kontenrollen

ROLLEN	BESCHREIBUNG
Unternehmensadministrator	Kontrolliert das gesamte Unternehmen und verfügt über administrative Rechte für alle Gruppen, Benutzer, Geräte und Richtlinien, unabhängig davon, wo sie sich innerhalb des Unternehmens befinden.
Gruppenadministrator	Verfügt über administrative Rechte für alle Gruppen und deren Untergruppen, denen er zugewiesen wurde. **Hinweis** Diese Rechte gelten nicht für übergeordnete Gruppen, Gruppen auf derselben Hierarchieebene oder deren Untergruppen.
Unternehmensauthentifizierer	Wird dem Helpdesk-Personal zugewiesen, um Remote-Hilfe bereitzustellen. Dies kann der Fall sein, wenn ein Benutzer sich an den Helpdesk wenden muss, weil das Kennwort vergessen wurde oder ein technisches Problem vorliegt. Unternehmensauthentifizierer haben Berechtigungen, die über das gesamte Unternehmen konfiguriert werden können.
Gruppenauthentifizierer	Ähnlich wie Unternehmensauthentifizierer, aber nur auf die Gruppenebene beschränkt.

Rollen	Beschreibung
Benutzer	Für Endbenutzer, die Endpunkt-Clients verwenden, die jedoch keine Administrator- oder Authentifiziererverantwortlichkeiten haben.

Zugriffssteuerung nach Anwendung

Authentifizierung und Zugriffskontrolle sind in jedem Unternehmen wichtig. Full Disk Encryption beschränkt den Systemzugriff beim Systemstart sowie den Datei- und Ordnerzugriff, wenn der Benutzer beim Betriebssystem angemeldet ist. FileArmor, KeyArmor und PolicyServer ermöglichen durch Zwei-Faktor-Authentifizierung denselben Grad an Sicherheit und Zugriffssteuerung.

Jede Endpoint Encryption Anwendung bietet unterschiedliche Merkmale und Steuerungsebenen.

Tabelle 1-10. Authentifizierungssteuerung nach Anwendung

Anwendung	Steuerung
PolicyServer	Anwendungszugriff auf die Management-Konsole.
Full Disk Encryption	Authentifizierungssteuerung vor dem Starten von Windows.
FileArmor	Zugriffssteuerung auf Datei- und Ordnerebene bei gestartetem Betriebssystem.
KeyArmor	Gerätesteuerung für Zugriff auf verschlüsselte Inhalte auf Wechseldatenträgern.

Authentifizierungsoptionen nach Anwendung

TABELLE 1-11. Für Endpunkt-Clients verfügbare Authentifizierungsoptionen

PRODUKT	AUTHENTIFIZIERUNGSOPTIONEN					
	FESTES KENNWORT	DOMÄNENKENNWORT	SMARTCARD	PIN	RSA	COLORCODE
PolicyServer	Ja	Ja	Ja	Nein	Nein	Nein
Full Disk Encryption	Ja	Ja	Ja	Ja	Nein	Ja
FileArmor	Ja	Ja	Ja	Ja	Nein	Ja
KeyArmor	Ja	Nein	Ja	Ja	Ja	Ja

Sicherheitsoptionen

Wenn Benutzer sich nicht authentifizieren können, werden sie aufgefordert, ihre Anmeldedaten erneut einzugeben. Abhängig von den Richtlinieneinstellungen führen zu viele aufeinanderfolgende nicht erfolgreiche Authentifizierungsversuche zu einer Verzögerung des nächsten Anmeldversuchs, zu einer Sperrung oder zum Löschen aller Daten vom Endpunkt.

TABELLE 1-12. Sicherheitsoptionen für die Authentifizierung

SICHERHEITSOPTION	BESCHREIBUNG
Zeitverzögerung	Das Gerät wird gesperrt, und es können keine Authentifizierungsversuche durchgeführt werden, bis die Dauer der Sperre abläuft. • Stellen Sie sicher, dass die Anmeldedaten richtig sind. • Verwenden Sie die Selbsthilfe (falls verfügbar), damit Sie nicht bis zum Ablauf der Zeitverzögerung warten müssen.

SICHERHEITSOPTION	BESCHREIBUNG
Remote-Authentifizierung erforderlich	Das Gerät ist gesperrt. • Stellen Sie sicher, dass die Anmeldedaten richtig sind. • Wenden Sie sich an den Administrator, um die Remote-Hilfe zu verwenden und das Gerät zu entsperren. Weitere Informationen finden Sie unter *Remote-Hilfe auf Seite 1-19*.
Gerät wird gelöscht	Alle Daten werden vom Gerät entfernt.

Authentifizierungsmethode

Endpoint Encryption bietet mehrere Authentifizierungsmethoden. Die für den Endpunkt-Client verfügbaren Methoden werden von PolicyServer bestimmt.

TABELLE 1-13. Unterstützte Authentifizierungsmethoden

AUTHENTIFIZIERUNGSTYP	BESCHREIBUNG
Domänenauthentifizierung	SSO (Single-Sign-On) mit Hilfe von Active Directory.
Festes Kennwort	Eine Zeichenfolge aus Zeichen, Ziffern und Symbolen.
PIN	Eine standardmäßige persönliche Identifikationsnummer.
ColorCode™	Eine Farbenfolge wird als Kennwort verwendet.
Smartcard	Eine physische Karte wird in Verbindung mit einer PIN oder einem festen Kennwort verwendet.
Selbsthilfe	Kombinationen aus Fragen und Antworten, mit denen ein Benutzer ein vergessenes Kennwort zurücksetzen kann, ohne sich an den Support zu wenden.
Remote-Hilfe	Interaktive Authentifizierung für Benutzer, die ihre Anmeldedaten vergessen haben, oder für Geräte, deren Richtlinien nicht innerhalb eines bestimmten Zeitraums synchronisiert wurden.

Domänenauthentifizierung

Die Domänenauthentifizierung mit Hilfe von Active Directory unterstützt Single-Sign-On (SSO). Benutzer müssen nur einmal Anmeldedaten eingeben, um sich bei Full Disk Encryption zu authentifizieren, bei Windows anzumelden und auf FileArmor zuzugreifen.

Voraussetzungen

Zur nahtlosen Integration vergewissern Sie sich, dass die folgenden Anforderungen erfüllt werden:

- Alle Geräte befinden sich in derselben Domäne wie der PolicyServer.
- Der in Active Directory konfigurierte Benutzername stimmt genau mit dem Benutzernamen in PolicyServer überein, auch hinsichtlich der Groß- und Kleinschreibung.
- Der Benutzername befindet sich innerhalb einer PolicyServer Gruppe und die Richtlinie "Domänenauthentifizierung" ist auf **Ja** festgelegt.
- Die Richtlinien unter **Allgemein** > **Netzwerkanmeldung** (Host-Name, Domänenname) sind auf Grundlage der LDAP- oder Active Directory-Servereinstellungen richtig konfiguriert.



Hinweis

Weitere Informationen zum Konfigurieren der LDAP- und Active Directory-Einstellungen finden Sie unter *Active Directory Synchronisierung auf Seite 1-21*.

Feste Kennwörter

Feste Kennwörter sind die häufigste Authentifizierungsmethode. Ein festes Kennwort wird vom Benutzer angelegt und kann fast alles sein. Administratoren können für feste Kennwörter Einschränkungen festlegen, um sicherzustellen, dass diese nicht leicht missbraucht werden können.

PIN

Eine persönliche Identifikationsnummer (PIN) ist eine andere häufige Identifikationsmethode. Wie ein festes Kennwort wird eine PIN vom Benutzer angelegt und kann fast alles sein. Administratoren können für PIN-Kombinationen Einschränkungen festlegen wie für feste Kennwörter.

ColorCode

ColorCode™ist eine einzigartige Authentifizierungsmethode, bei deren Entwicklung eine leichte Merkfähigkeit und schnelle Eingabe im Vordergrund standen. Anstelle der Verwendung von Ziffern und Buchstaben für ein Kennwort besteht die ColorCode-Authentifizierung aus einer vom Benutzer erzeugten Farbfolge (z. B. rot, rot, blau, gelb, blau, grün).

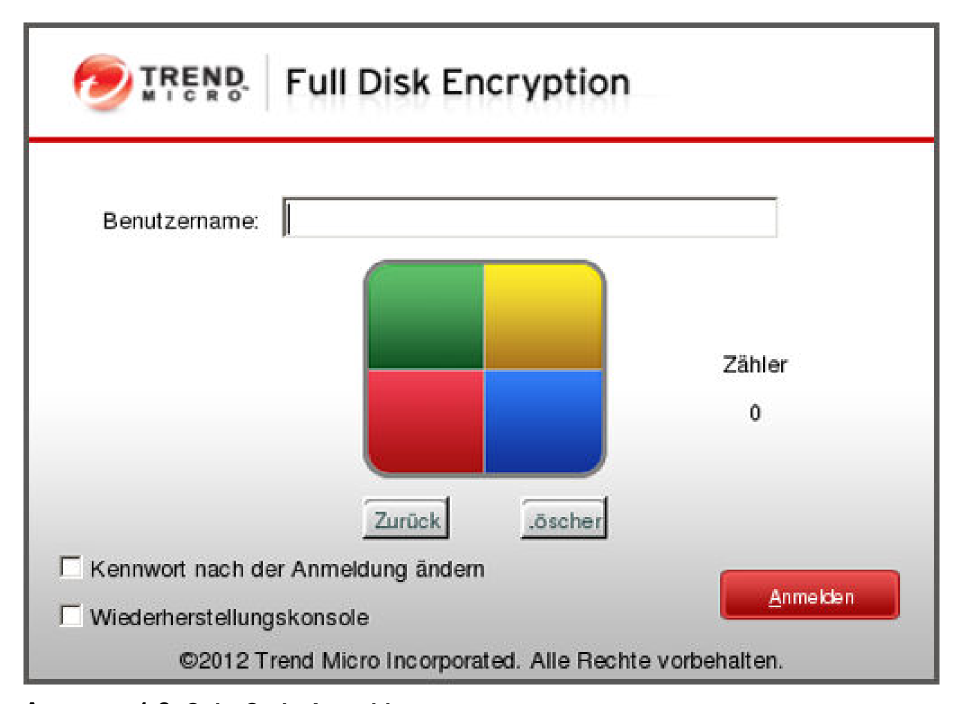


ABBILDUNG 1-2. ColorCode-Anmeldung

SmartCard

Die Smartcard-Authentifizierung erfordert sowohl eine PIN als auch eine physische Karte zur Bestätigung der Identität des Benutzers. Führen Sie die Smartcard vor der Eingabe der PIN ein.



Wichtig

Aktivieren Sie die folgende Richtlinie, um die Smartcard-Authentifizierung für alle Endpoint Encryption Clients zuzulassen: **Full Disk Encryption** > **PC** > **Anmelden** > **Token-Authentifizierung**.

Selbsthilfe

Benutzer verwenden die Selbsthilfe zur Authentifizierung, wenn sie ihre Anmeldedaten vergessen haben. Die Benutzer werden aufgefordert, die vordefinierten persönlichen Herausforderungsfragen der Selbsthilfe zu beantworten. Die Selbsthilfe kann anstelle von festen Kennwörtern oder anderen Authentifizierungsmethoden verwendet werden.



Wichtig

PolicyServer muss für die Selbsthilfe-Authentifizierung konfiguriert sein. Weitere Informationen finden Sie unter *Richtlinien verstehen auf Seite 3-1*.



Warnung!

Für Endpunkt-Clients können maximal sechs Fragen angezeigt werden. Erstellen Sie nicht mehr als sechs Fragen in PolicyServer, sonst können sich die Benutzer nicht anmelden.

Remote-Hilfe

Verwenden Sie die Remote-Hilfe, wenn der Zugriff eines Benutzers auf einen Endpunkt-Client gesperrt wurde, weil zu viele Anmeldeversuche fehlgeschlagen sind oder weil die Zeitspanne seit der letzten PolicyServer Synchronisierung zu lang ist.

Setzen Sie die Aktion in den Richtlinien jeder Anwendung auf **Remote-Authentifizierung**.

TABELLE 1-14. Richtlinien mit Auswirkungen auf die Authentifizierung für die Remote-Hilfe

RICHTLINIE	BESCHREIBUNG
Anmelden > **Zeitraum bis Kontosperrung**	Die Anzahl von Tagen, die ein Gerät ohne Kommunikation mit PolicyServer sein kann, bevor die Kontosperraktion ausgeführt wird.
Anmelden > **Kontosperraktion**	Die Aktion, die durchgeführt wird, wenn der angegebene Zeitraum abgelaufen ist. Mögliche Aktionen sind Löschen und Remote-Authentifizierung.
Anmelden > **Zulässige Anzahl fehlgeschlagener Anmeldeversuche**	Die Anzahl der zulässigen fehlgeschlagenen Anmeldeversuche, bevor die Aktion zur Gerätesperrung ausgeführt wird.
Anmelden > **Aktion zur Gerätesperrung**	Die Aktion, die durchgeführt wird, wenn der in der Richtlinie "Zulässige Anzahl fehlgeschlagener Anmeldeversuche" festgelegte Wert überschritten wurde. Mögliche Aktionen sind Zeitverzögerung, Löschen und Remote-Authentifizierung.

Neue Funktionen in Endpoint Encryption 3.1.3

Trend Micro Endpoint Encryption 3.1.3 bietet die folgenden Verbesserungen:

Unterstützung mehrerer Sprachen

Endpoint Encryption bietet jetzt Unterstützung für folgende Sprachen:

TABELLE 1-15. Unterstützte Sprachen

PRODUKT	SPRACHEN		
	SPANISCH	FRANZÖSISCH	DEUTSCH
Full Disk Encryption	Ja	Ja	Ja

Produkt	**Sprachen**		
	Spanisch	**Französisch**	**Deutsch**
FileArmor	Ja	Ja	Ja
PolicyServer	Ja	Ja	Ja
KeyArmor	Nein	Nein	Nein

Active Directory Synchronisierung

Endpoint Encryption unterstützt jetzt die Kontensynchronisierung zwischen Active Directory und PolicyServer. Active Directory kann für Single-Sign-On bei allen Endpunkt-Client-Anwendungen eingesetzt werden.

Im Endpoint Encryption Installationshandbuch finden Sie detaillierte Anweisungen zum Konfigurieren von PolicyServer für die AD-Synchronisierung. Die Installationshandbuch ist unter folgender Adresse verfügbar:

http://docs.trendmicro.com/de-de/enterprise/endpoint-encryption.aspx

Verbesserungen in PolicyServer 3.1.3

- Das PolicyServer Installationsprogramm ermöglicht eine Testlizenz, die nach 30 Tagen abläuft. Der Unternehmensname und das Konto für den Unternehmensadministrator werden im Rahmen der Installation konfiguriert.
- Die Portnummer für Web-Services kann jetzt während der Installation festgelegt werden.
- Zur Erhöhung der Sicherheit verfügt PolicyServer nun über einen Client-Web-Service, der es allen Clients ermöglicht, mit Hilfe dieser neuen Schnittstelle eine Verbindung zu PolicyServer herzustellen.
- Verbessertes Nachschlagen und Benennen von Richtlinien.
- Verbesserte Audit-Protokolle.
- Ein neuer Papierkorb-Knoten ermöglicht es Administratoren, gelöschte Benutzer und Geräte wiederherzustellen.

- Allgemeine Richtlinien ermöglichen nun ein einfaches Verschieben von Richtlinienänderungen von der übergeordneten Ebene zu Untergruppen.

Full Disk Encryption 3.1.3 - Verbesserungen

Neue Funktionen

- OPAL 2 wird nun unterstützt.
- Windows 8 wird nun auf Nicht-UEFI-Geräten unterstützt.
- Richtlinien werden jetzt automatisch mit PolicyServer synchronisiert, wenn ein Gerät die Preboot-Anmeldung lädt.
- Der Austausch von Kennwörtern auf Geräten in derselben PolicyServer Gruppe (für Geräte mit gemeinsamen Kennwörtern) wird nun unterstützt.
- Nicht verwaltete Installationen unterstützen nun vollständig die Hardware- und die Software-basierte Verschlüsselung.
- Konsolenbasierter Preboot-Modus funktioniert nun für nicht unterstützte Anzeigenkonfigurationen.

Einfache Installation

- Es gibt nun ein gemeinsames Installationsprogramm für Software- und Hardware-basierte Verschlüsselung (Seagate OPAL und DriveTrust). Dieses Installationsprogramm unterstützt auch 32- und 64-Bit-Betriebssysteminstallationen.
- Verbesserte Vorinstallations- und Fehler-/Protokoll-Prüfberichte.
- Full Disk Encryption kann nun ohne Verschlüsselung und ohne Preboot (über Richtlinieneinstellung) installiert werden. Dies ermöglicht eine bessere Kontrolle eines schrittweisen Rollout zur Verteilung von Software, erlaubt eine Preboot-Authentifizierung und schaltet die Verschlüsselung ein.

Verbesserungen bei Management und Administration

- Zugriff auf die Wiederherstellungskonsole in Windows und Preboot.

- Einfache Aktualisierung der PolicyServer Informationen und Neuzuweisung eines Geräts an den originalen PolicyServer oder einen neuen PolicyServer.
- Stabilere Reparatur-CD
- Skriptgesteuerte Deinstallationen



Kapitel 2

Erste Schritte mit PolicyServer

Vor der Konfiguration von PolicyServer für die zentrale Verwaltung von Endpunkt-Clients sollten PolicyServer Dienste, Datenbanken und PolicyServer MMC bereits installiert sein. Detaillierte Anweisungen zum Einrichten von PolicyServer Dienste, Datenbanken und PolicyServer MMC finden Sie im Installationshandbuch für Endpoint Encryption. Die Installationshandbuch ist unter folgender Adresse verfügbar:

http://docs.trendmicro.com/de-de/enterprise/endpoint-encryption.aspx

Dieses Kapitel umfasst folgende Themen:

- *Erste Authentifizierung auf Seite 2-2*
- *Einführung in PolicyServer auf Seite 2-2*
- *Mit Gruppen und Benutzern arbeiten auf Seite 2-5*
- *Richtliniensteuerelemente verstehen auf Seite 2-14*
- *Anwendungen aktivieren auf Seite 2-18*

Erste Authentifizierung

Der Unternehmensname und das Konto für den Unternehmensadministrator wurden im Rahmen der Installation konfiguriert. PolicyServer funktioniert normal mit allen Client-Anwendungen, unbegrenzten Geräten und 100 verfügbaren Benutzern für einen Testzeitraum von 30 Tagen. Wenden Sie sich nach 30 Tagen an den Technischen Support, um eine Lizenzdatei zu erhalten. Nach Ablauf der Testzeitraums können sich Benutzer/Geräte weiterhin anmelden.

Diese Aufgabe erklärt den Import der Lizenzdatei und die anschließende Anmeldung bei PolicyServer. Sie wird in der Regel als Textdatei bereitgestellt.

Prozedur

1. Öffnen Sie PolicyServer MMC.
2. Navigieren Sie zu **Datei** > **Lizenz importieren**.
3. Geben Sie den Code zum Entsperren der Lizenzdatei ein.
4. Navigieren Sie zur Lizenzdatei, und klicken Sie anschließend auf **Update**.
5. Geben Sie die Angaben in der Lizenzdatei ein: Unternehmen, Benutzername, Kennwort sowie IP-Adresse oder Hostname vom PolicyServer.
6. Klicken Sie auf **Anmelden**.

Einführung in PolicyServer

PolicyServer verwendet eine Microsoft Management-Konsole (MMC). PolicyServer hat eine hierarchische Struktur, die administrativen Verantwortlichkeiten verteilt und eine zentralisierte Steuerung aufrecht erhält, wenn:

- Parameter für Sicherheitsrichtlinien definiert werden
- Benutzer, Geräte und Gruppen (Offline-Gruppen) verwaltet werden
- Endpunktanwendungen aktiviert/deaktiviert werden

Verwenden Sie die Audit- und Berichterstellungsfunktionen von PolicyServer MMC, um die Sicherheitsinfrastruktur zu überwachen und die Einhaltung von Bestimmungen zu gewährleisten.

PolicyServer MMC-Benutzeroberfläche

Die Benutzeroberfläche von PolicyServer MMC besteht aus den folgenden Fensterbereichen:

TABELLE 2-1. PolicyServer MMC-Benutzeroberfläche

FENSTER	BESCHREIBUNG
Linker Fensterbereich (1)	Im linken Fensterbereich können Sie Benutzer, Gruppen, Richtlinien, Geräte und Anwendungen anzeigen. Erweitern Sie die oberste Ebene, um verschachtelte Elemente innerhalb der Baumstruktur zu verwalten. Durch geöffnete Elemente wird der Inhalt im Ergebnisfenster aktualisiert.
Rechter Fensterbereich (2)	Im rechten Fensterbereich können Sie Richtlinien, Benutzerinformationen sowie Gruppeninformationen ändern. Das aktuell ausgewählte Strukturelement wird im Ergebnisfenster angezeigt. Das genaue Format der im Ergebnisfenster angezeigten Informationen hängt vom Element ab, das in der Baumstruktur ausgewählt wurde.

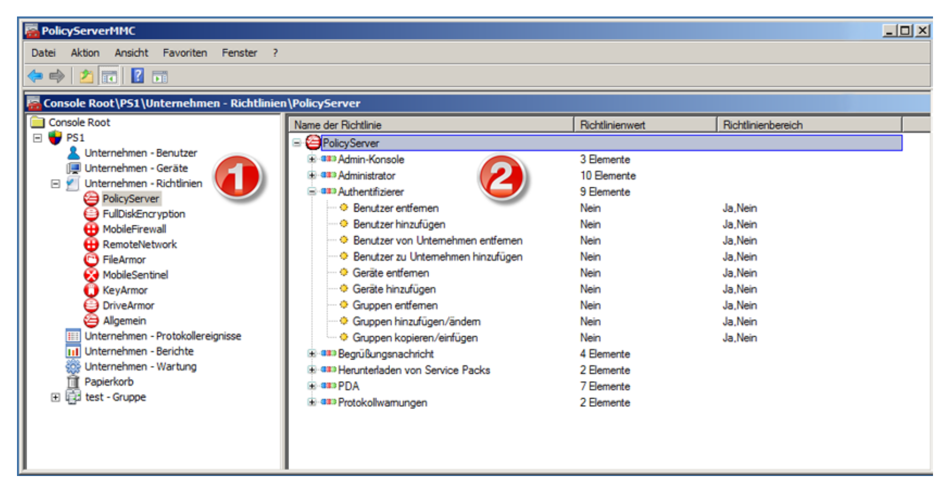


ABBILDUNG 2-1. PolicyServer MMC-Benutzeroberfläche

Die Baumstruktur im linken Fensterbereich umfasst eine Reihe unterschiedlicher Knoten. In der folgenden Tabelle werden die einzelnen Knoten beschrieben:

TABELLE 2-2. Baumstrukturhierarchie in PolicyServer MMC

KNOTEN	ZWECK
Unternehmen - Benutzer	Zeigen Sie alle Administratoren, Authentifizierer und Benutzer im gesamten Unternehmen an. Wenn Sie die Gruppenzugehörigkeit anzeigen möchten, öffnen Sie die Gruppe und klicken Sie auf **Benutzer**.
Unternehmen - Geräte	Zeigen Sie alle Instanzen der Endpunkt-Clients und die Geräte, über die sie eine Verbindung herstellen, an. Wenn Sie die Gruppenzugehörigkeit anzeigen möchten, öffnen Sie die Gruppe und klicken Sie auf **Geräte**.
Unternehmen - Richtlinien	Mit diesem Knoten steuern Sie, ob Endpunktanwendungen eine Verbindung zu PolicyServer herstellen können. Außerdem können Sie alle Unternehmensrichtlinien verwalten. Gruppenrichtlinien setzen Unternehmensrichtlinien außer Kraft.

KNOTEN	ZWECK
Unternehmen - Protokollereignisse	Zeigen Sie alle Protokolleinträge für das Unternehmen an.
Unternehmen - Berichte	Verwalten Sie die verschiedenen Berichte und Warnungen. Berichte nur für Gruppen sind nicht verfügbar.
Unternehmen - Wartung	Verwalten Sie Anwendungs-Plug-ins von PolicyServer MMC.
Papierkorb	Zeigen Sie gelöschte Benutzer und Geräte an.
Gruppen	Verwalten Sie Benutzer, Gruppen, Richtlinien und Protokollereignisse für eine Auswahl von Benutzern.

Mit Gruppen und Benutzern arbeiten

In diesem Abschnitt wird der Einstieg in Gruppen und Benutzer in Endpoint Encryption erläutert. Definieren Sie zunächst die Benutzer und Gruppen und weisen Sie die Benutzer anschließend den Gruppen zu. Sie können neue Benutzer auch direkt zu einer Gruppe hinzufügen. Es ist mindestens eine Top-Gruppe erforderlich.

Empfehlungen für die Benutzer- und Gruppenstruktur:

- Folgen Sie beim Konfigurieren einer Gruppenstruktur der Struktur von Active Directory.
- Erstellen Sie eine neue Gruppe, wann immer unterschiedliche Richtlinien zwischen Benutzergruppen bestehen. Wenn z. B. eine Gruppe eine Domänenauthentifizierung und eine andere ein festes Kennwort erfordert, werden zwei separate Richtliniengruppen benötigt.
- Erstellen Sie mehrere Gruppen, um den Zugriff auf Geräte innerhalb einer Gruppe zu minimieren. Alle Mitglieder einer Gruppe sind berechtigt, auf alle Geräte in dieser Gruppe zuzugreifen.

Benutzer und Gruppen definieren

Definieren Sie alle Rollen und Gruppenzugehörigkeiten, bevor Sie Benutzer oder Gruppen zu PolicyServer hinzufügen.

1. Identifizieren Sie Unternehmensadministratoren/-authentifizierer.
2. Erstellen Sie Unternehmensadministratoren/-authentifizierer.
3. Identifizieren Sie Gruppen.
4. Erstellen Sie Gruppen.
5. Identifizieren Sie Gruppenadministratoren/-authentifizierer.
6. Erstellen Sie Gruppenadministratoren/-authentifizierer.
7. Identifizieren Sie die Benutzer, die Sie jeder Gruppe zuweisen.
8. Importieren oder erstellen Sie neue Benutzer für jede Gruppe.

Top-Gruppe hinzufügen

Gruppen vereinfachen die Verwaltung von aktivieren Anwendungen, Benutzern, Richtlinien, Untergruppen und Geräten. Die Top-Gruppe ist die Gruppe auf der höchsten Stufe.



Hinweis

Unternehmensadministrator- oder -authentifiziererkonten können nicht zu Gruppen hinzugefügt werden. Um einen Gruppenadministrator zu erstellen, fügen Sie einen Benutzer hinzu und ändern Sie seine Berechtigungen innerhalb der Gruppe.

Prozedur

1. Klicken Sie mit der rechten Maustaste im linken Fenster auf den Namen des Unternehmens und klicken Sie anschließend auf **Top-Gruppe hinzufügen**.

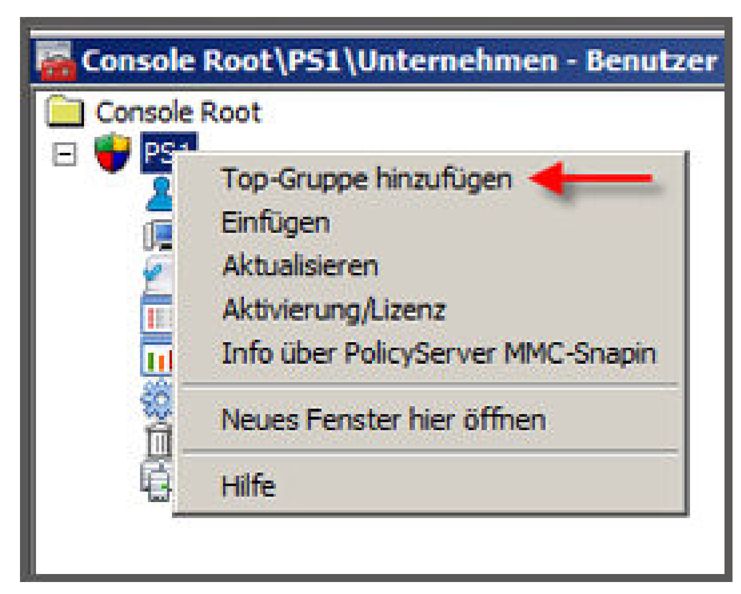


ABBILDUNG 2-2. Top-Gruppe hinzufügen

Das Fenster **Neue Gruppe hinzufügen** wird angezeigt.

2. Geben Sie den Namen und eine Beschreibung der Gruppe an.

3. Wählen Sie **Altgeräte unterstützen** nur aus, wenn Sie Altgeräte verwenden, die die Unicode-Codierung nicht unterstützen. Einige Altgeräte sind möglicherweise nicht in der Lage, unter Verwendung von Unicode mit PolicyServer zu kommunizieren. Weisen verschiedenen Gruppen Unicode und Altgeräte hinzu.

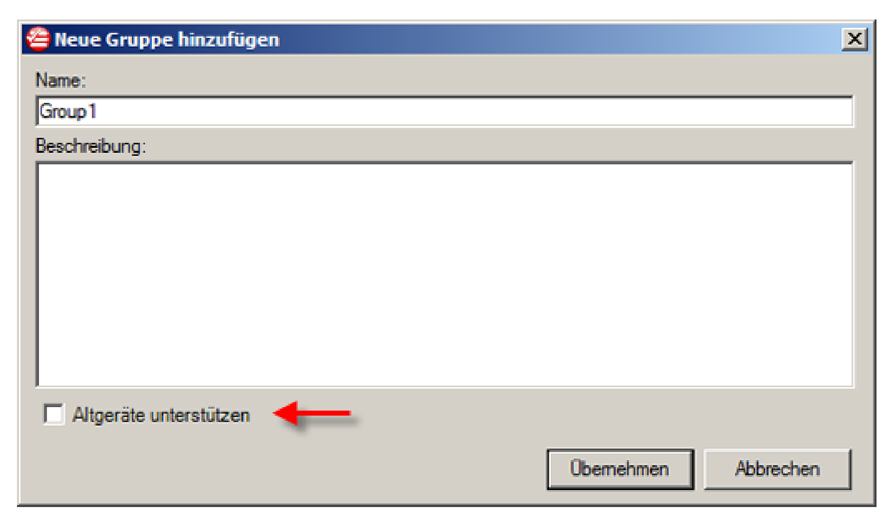


ABBILDUNG 2-3. Neue Gruppe hinzufügen

4. Klicken Sie auf **Übernehmen**.

5. Wenn die Bestätigungsmeldung angezeigt wird, klicken Sie auf **OK**.

   Die neue Gruppe wird zur Baumstruktur im linken Fensterbereich hinzugefügt.

Neuen Benutzer zu einer Gruppe hinzufügen


Hinweis

- Beim Hinzufügen eines Benutzers zum Unternehmen wird der Benutzer keiner Gruppe zugewiesen.
- Beim Hinzufügen eines Benutzers zu einer Gruppe wird der Benutzer zur Gruppe und zum Unternehmen hinzugefügt.

Prozedur

1. Erweitern Sie die Gruppe und öffnen Sie **Benutzer**.

2. Klicken Sie mit der rechten Maustaste auf den leeren Bereich im rechten Fenster und wählen Sie **Neuen Benutzer hinzufügen** aus.

   Das Fenster **Neuen Benutzer hinzufügen** wird angezeigt.

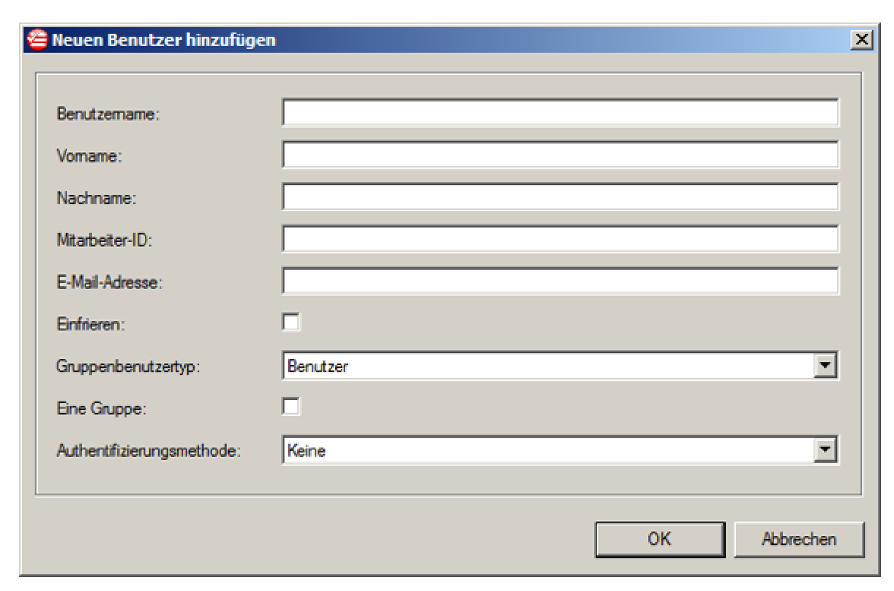


ABBILDUNG 2-4. Fenster "Neuen Benutzer hinzufügen"

3. Geben Sie die Benutzerinformationen ein. Benutzername, Vorname und Nachname sind erforderlich.

4. Wählen Sie nur **Einfrieren** aus, wenn das Konto vorübergehend deaktiviert werden soll. Wenn das Konto eingefroren ist, kann sich der Benutzer nicht an Geräte anmelden.

5. Verwenden Sie das Feld **Gruppenbenutzertyp**, um die Berechtigungen des neuen Kontos festzulegen. Administratoren und Authentifizierer für das Unternehmen können nicht zu Gruppen hinzugefügt werden.

6. Wählen Sie **Eine Gruppe** aus, um die Mitgliedschaft des Benutzers in mehreren Gruppen zu deaktivieren.

7. Wählen Sie die **Authentifizierungsmethode**.



Hinweis

Die Standardauthentifizierungsmethode für Benutzer lautet **Keine**.

8. Klicken Sie auf **OK**.

   Der neue Benutzer wird der ausgewählten Gruppe **und** zum Unternehmen hinzugefügt. Der Benutzer kann sich jetzt ein Gerät anmelden.

Neuen Unternehmensbenutzer hinzufügen



Hinweis

- Beim Hinzufügen eines Benutzers zum Unternehmen wird der Benutzer keiner Gruppe zugewiesen.
- Beim Hinzufügen eines Benutzers zu einer Gruppe wird der Benutzer zur Gruppe und zum Unternehmen hinzugefügt.

Prozedur

1. Erweitern Sie das Unternehmen und öffnen Sie **Benutzer**.
2. Klicken Sie mit der rechten Maustaste auf den leeren Bereich im rechten Fenster und wählen Sie **Benutzer hinzufügen** aus.

   Das Fenster **Neuen Benutzer hinzufügen** wird angezeigt.

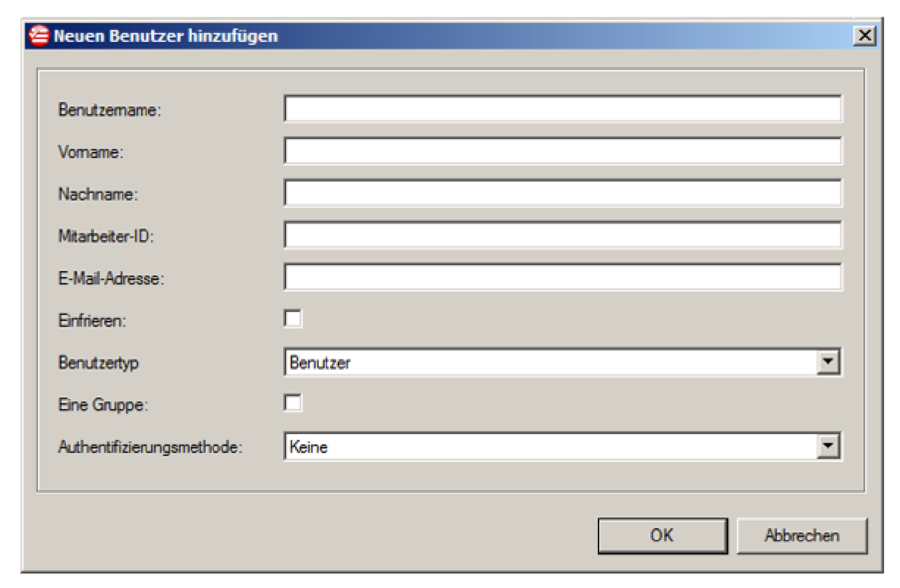


ABBILDUNG 2-5. Fenster "Neuen Benutzer hinzufügen"

3. Geben Sie die Benutzerinformationen ein. Benutzername, Vorname und Nachname sind erforderlich.

4. Wählen Sie nur **Einfrieren** aus, wenn das Konto vorübergehend deaktiviert werden soll. Wenn das Konto eingefroren ist, kann sich der Benutzer nicht an Geräte anmelden.

5. Verwenden Sie das Feld **Benutzertyp**, um die Berechtigungen des neuen Kontos festzulegen. Administratoren und Authentifizierer für das Unternehmen können nicht zu Gruppen hinzugefügt werden.

6. Wählen Sie **Eine Gruppe** aus, um die Mitgliedschaft des Benutzers in mehreren Gruppen zu deaktivieren.

7. Wählen Sie die **Authentifizierungsmethode**.



Hinweis

Die Standardauthentifizierungsmethode für Benutzer lautet **Keine**.

8. Klicken Sie auf **OK**.

Der neue Benutzer wird PolicyServer Enterprise hinzugefügt. Der Benutzer kann erst ein Gerät anmelden, wenn er/sie einer Gruppe hinzugefügt wird.

Vorhandenen Benutzer zu einer Gruppe hinzufügen

Ein Benutzer kann zu mehreren Gruppen hinzugefügt werden.

Prozedur

1. Erweitern Sie die Gruppe im linken Fenster und klicken Sie anschließend auf **Benutzer**.
2. Klicken Sie mit der rechten Maustaste auf den leeren Bereich im rechten Fenster und wählen Sie **Vorhandenen Benutzer hinzufügen** aus.

   Das Fenster **Benutzer zu Gruppe hinzufügen** wird angezeigt.

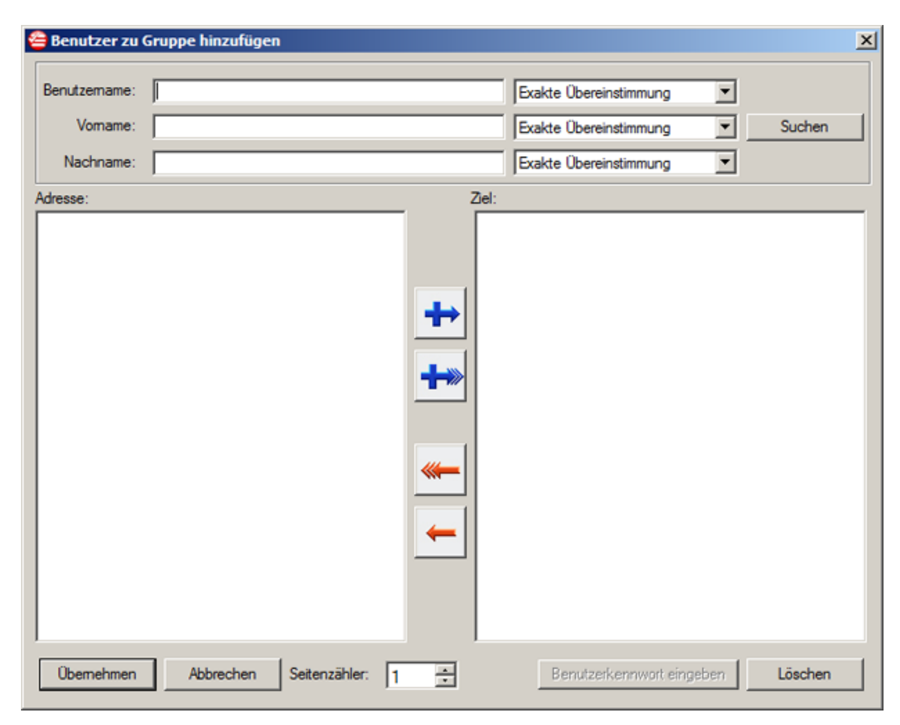


ABBILDUNG 2-6. Fenster "Vorhandenen Benutzer zu Gruppe hinzufügen"

3. Geben Sie die Benutzerdetails ein und klicken Sie dann auf **Suchen**.

   Wird eine Übereinstimmung gefunden, werden im Feld **Quelle** Konten angezeigt.

4. Wählen Sie Benutzerkonten aus der Liste aus und klicken Sie auf den **blauen Pfeil**, um sie hinzuzufügen. Weitere Steuerelemente finden Sie unter *Tabelle 2-3: Symbole zum Hinzufügen/Entfernen von Benutzern auf Seite 2-13*.

TABELLE 2-3. Symbole zum Hinzufügen/Entfernen von Benutzern

ZENTRALE SYMBOLE	BESCHREIBUNG
	Fügt einen einzelnen ausgewählten Benutzer zum Feld **Ziel** hinzu.

Zentrale Symbole	Beschreibung
	Fügt alle gefundenen Benutzer basierend auf Suchkriterien zum Feld **Ziel** hinzu.
	Löscht einen einzelnen ausgewählten Benutzer im Feld **Ziel**.
	Löscht alle Benutzer im Feld **Ziel**.

5. So ändern Sie ein Benutzerkennwort:

a. Markieren Sie den Benutzer im Feld **Ziel**.

b. Klicken Sie im unteren Fensterbereich auf **Benutzerkennwort eingeben**.

c. Geben Sie im anschließend angezeigten Fenster die Authentifizierungsmethode für den Benutzer an.

d. Klicken Sie auf **Übernehmen**.

6. Klicken Sie auf **Übernehmen**.

Der Benutzer wird zur Gruppe hinzugefügt. Wenn dies die einzige Gruppe ist, zu der der Benutzer gehört, kann sich der Benutzer nun beim Endpunkt-Client anmelden.

Richtliniensteuerelemente verstehen

Nachdem Sie alle Benutzer und Gruppen im Unternehmen eingerichtet haben, legen Sie Richtlinien für das Unternehmen oder die Gruppe fest. Jede Gruppe in der Baumstruktur im linken Fensterbereich (ob Top-Gruppe oder Untergruppe) enthält mindestens einen Richtlinienordner für Endpunktanwendungen.

Weitere Informationen zur Benutzeroberfläche von PolicyServer finden Sie unter *PolicyServer MMC-Benutzeroberfläche auf Seite 2-3*.



Hinweis

Richtlinien können auf Unternehmens- oder Gruppenebene aktiviert bzw. deaktiviert werden. Weitere Informationen finden Sie unter *Mit Richtlinien arbeiten auf Seite 3-2*.

Optische Indikatoren für Richtlinien

Farbige Kreise neben jeder Richtlinie geben den Status der jeweiligen Richtlinie an.

TABELLE 2-4. Richtlinienindikatoren

INDIKATOR	BESCHREIBUNG
	Der Richtlinienwert wird von der übergeordneten Gruppe oder vom Unternehmen übernommen.
	Eine Richtlinie wird für die Gruppe geändert.
	Die Richtlinie enthält möglicherweise mehrere Werte-Arrays.
	Die Richtlinie hat mindestens eine Unterrichtlinie.

Felder und Schaltflächen für Richtlinien

Mit den unten angegebenen Feldern und Schaltflächen können Sie Richtlinienelemente steuern. Alle geänderten Werte werden auf die Untergruppen der jeweiligen Gruppe übertragen. Abhängig vom Element, das von der Richtlinie gesteuert wird, sind bestimmte Felder nicht vorhanden.

TABELLE 2-5. Felder und Schaltflächen für Richtlinien

FELD/SCHALTFLÄCHE	BESCHREIBUNG	ÄNDERBAR?
OK	Speichert Änderungen in der ausgewählten Richtlinie.	n. v.
Beschreibung	Beschreibt die ausgewählte Richtlinie.	Nein
Richtlinienbereich	Zeigt den zulässigen Wertebereich für die ausgewählte Richtlinie an.	Ja
Richtlinienwert	Zeigt abhängig von der Richtlinie den aktuellen Wert der ausgewählten Richtlinie an (ob eine Zeichenfolge, eine Zahl oder eine Serie von Einträgen enthalten ist).	Ja
Richtlinienmehrfachwert	Gibt an, ob diese Richtlinie mehrere Male für verschiedene Einstellungen verwendet werden kann (z. B. mehrere "Falls gefunden"-Zeichenfolgen).	Nein
Name der Richtlinie	Zeigt den Namen der ausgewählten Richtlinie an.	Nein
Richtlinientyp	Gibt die Kategorie der ausgewählten Richtlinie an.	Nein
Unternehmensgesteuert	Änderungen an dieser Richtlinie werden auf dieselbe Richtlinie auf Unternehmensebene gespiegelt.	Ja
In Untergruppen speichern	Verteilt die Richtlinieneinstellungen auf dieselben Richtlinien in allen Untergruppen.	Ja

Richtlinien ändern

PolicyServer verfügt über mehrere allgemeine Fenster zum Ändern von Richtlinien. Je nachdem, welche Elemente die Richtlinie steuert und welche Parameter erforderlich sind, stehen unterschiedliche Arten der Eingabe zur Verfügung. Die Bearbeitung verschiedener Richtlinien erfordert auch unterschiedliche Schritte. Mit dieser Aufgabe wird ein allgemeiner Überblick über die Bearbeitung einer Richtlinie bereitgestellt.

Weitere Informationen zur Bearbeitung von Richtlinien, einschließlich Erläuterungen zur Konfiguration unterschiedlicher Richtlinientypen, finden Sie unter *Richtlinienverwaltung auf Seite 3-2*.

Prozedur

1. Erweitern Sie den Knoten **Unternehmen**.
2. Wählen Sie die zu ändernde Richtlinienebene aus:
   a. Für Richtlinien auf Unternehmensebene erweitern Sie **Unternehmen - Richtlinien**.
   b. Für Richtlinien auf Gruppenebene erweitern Sie den **Gruppennamen** und anschließend die **Richtlinien**.
3. Öffnen Sie die spezifische Anwendung oder wählen Sie **Allgemein** aus.

   Die Liste der Richtlinien wird im Ergebnisfenster angezeigt.

Name der Richtlinie	Richtlinienwert	Richtlinienbereich
PolicyServer		
Admin-Konsole	3 Elemente	
Rechtlicher Hinweis		
Zeitüberschreitung der Konsole	20	1 - 60
Zulässige Anzahl fehlgeschlagener Anmeldeversuche	0	0 - 100
Administrator	10 Elemente	
Authentifizierer	9 Elemente	
Begrüßungsnachricht	4 Elemente	
Herunterladen von Service Packs	2 Elemente	
PDA	7 Elemente	
Protokollwarnungen	2 Elemente	

ABBILDUNG 2-7. Ändern einer Richtlinie

4. Navigieren Sie zu einer Richtlinie und doppelklicken Sie darauf, um das Editorfenster zu öffnen. In diesem Beispiel wird **Zeitüberschreitung der Konsole** verwendet.



ABBILDUNG 2-8. Editorfenster für die Richtlinie "Zeitüberschreitung der Konsole"

5. Nehmen Sie die für die Richtlinie entsprechenden Änderungen vor und klicken Sie anschließend auf **OK**.

Anwendungen aktivieren



Wichtig

Um eine ordnungsgemäße Kommunikation und Richtliniensynchronisierung sicherzustellen, muss die Endpoint Encryption Anwendung vor der Installation in PolicyServer aktiviert werden.

Prozedur

1. Melden Sie sich bei PolicyServer MMC an.

2. Klicken Sie auf **Unternehmen - Richtlinien**.

   Alle Anwendungen werden im rechten Fensterbereich angezeigt.

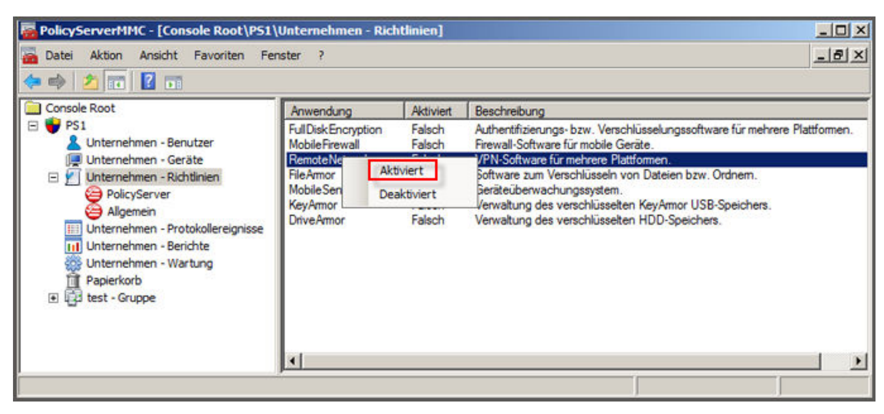


ABBILDUNG 2-9. Anwendungsaktivierung

3. Klicken Sie mit der rechten Maustaste auf die Anwendung und wählen Sie anschließend **Aktivieren** aus.



Hinweis

Um Full Disk Encryption verwenden zu können, müssen sowohl Full Disk Encryption als auch MobileSentinel Anwendungen aktiviert sein.

Die Anwendung wird von PolicyServer aktiviert und verwaltet.



Kapitel 3

Richtlinien verstehen

In diesem Kapitel wird die Verwendung von Richtlinien erläutert. Weiterhin werden ausführliche Informationen zu einzelnen Richtlinienwerten bereitgestellt. Informationen zum Verwalten von Benutzern, Gruppen und Geräten finden Sie unter *Arbeiten mit Gruppen, Benutzern und Geräten auf Seite 4-1*.

In diesem Kapitel werden die folgenden Themen erläutert:

- *Mit Richtlinien arbeiten auf Seite 3-2*
- *Richtlinienverwaltung auf Seite 3-2*
- *PolicyServer Richtlinien auf Seite 3-13*
- *Richtlinien für Full Disk Encryption auf Seite 3-19*
- *FileArmor Richtlinien auf Seite 3-27*
- *MobileSentinel Richtlinien auf Seite 3-32*
- *KeyArmor Richtlinien auf Seite 3-37*
- *DriveArmor Richtlinien auf Seite 3-41*
- *Allgemeine Richtlinien auf Seite 3-47*

Mit Richtlinien arbeiten

In diesem Abschnitt wird erläutert, wie verschiedene Fenster zum Ändern einer Richtlinie verwendet werden können. Das Verfahren zum Ändern aller Richtlinien wird hier jedoch nicht erläutert. Alle Richtlinien verfügen über Standardwerte. Die PolicyServer MMC verfügt über einen allgemeinen Satz an Fenstern, die zum Ändern einer Richtlinie verwendet werden können. Die eine Richtlinie weist ein Editorfenster auf, in dem mit der Richtlinie verbundene Zahlen, Bereiche und Werte geändert werden können, während eine andere Richtlinie über ein Fenster zum Ändern von Textzeichenfolgen verfügt.

Beachten Sie beim Verwalten von Richtlinien Folgendes:

- Richtlinien können nach Anwendung in jeder Gruppe konfiguriert werden.
- Richtlinienvererbung findet nur statt, wenn eine Untergruppe erstellt wird. Weitere Informationen zu Gruppenberechtigungen finden Sie unter *Arbeiten mit Gruppen auf Seite 4-2*.

Richtlinienverwaltung

Jede Gruppe in der linken Fensterstruktur (ob Top-Gruppe oder Untergruppe) enthält eine oder mehrere Ordner für Endpunkt-Anwendungsrichtlinien.

Das Ergebnisfenster im linken Fenster zeigt Steuerelemente für folgende Aktionen an:

- Anzeigen einer Liste mit Richtlinien und deren Werte
- Ändern einer Richtlinie mit dem Editor-Fenster
- Ausführen von Berichten und anderen Protokollereignissen
- Ausführen von Unternehmenswartung

Detaillierte Erläuterungen zur Benutzeroberfläche finden Sie unter *PolicyServer MMC-Benutzeroberfläche auf Seite 2-3*.

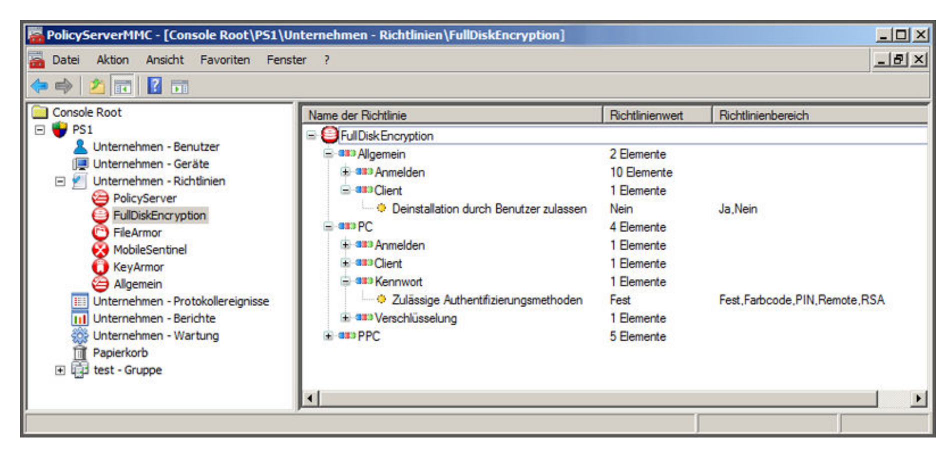


ABBILDUNG 3-1. PolicyServer MMC-Fenster

Richtlinie für Änderung auswählen

Prozedur

1. Navigieren Sie zu **Gruppenname** > **Richtlinien** > **Anwendungsname**.

   Beispiel: **Gruppe1** > **Richtlinien** > **Full Disk Encryption**.

2. Navigieren Sie zur spezifischen Richtlinie.

   Beispiel: **Allgemein** > **Client** > **Deinstallation durch Benutzer zulassen**.

3. Klicken Sie mit der rechten Maustaste auf die Richtlinie und wählen Sie **Eigenschaften** aus.

Richtlinien mit Bereichen bearbeiten

Ein Beispiel für die Bearbeitung von Richtlinien mit Bereichen stellt die Richtlinie **Zulässige Anzahl fehlgeschlagener Anmeldeversuche** dar. **Zulässige Anzahl**

fehlgeschlagener Anmeldeversuche steuert, ob ein Gerät gesperrt wird, wenn ein Benutzer die Anzahl der zulässigen Authentifizierungsverusche überschreitet.

Richtlinienwert bearbeiten

Richtlinienname:

Zulässige Anzahl fehlgeschlagener Anmeldeversuche

Richtlinienwert: 5

Richtlinienbereich

Minimum: 0 Maximum: 100

Der definierte Bereich ist 0 bis 100.

Richtlinienbeschreibung:

Geben Sie Anzahl der zulässigen fehlgeschlagenen Anmeldeversuche an, bevor die Aktion zur Gerätesperrung ausgeführt wird.

Unternehmensgesteuert

In Untergruppen speichern

OK Abbrechen

ABBILDUNG 3-2. Fenster "Richtlinie mit Bereichen"

Unter Verwendung der in den Feldern **Richtlinienbereich** definierten Parameter kann ein Administrator die Anzahl der fehlgeschlagenen Anmeldeversuche pro Benutzer im Feld **Richtlinienwert** angeben.

Prozedur

1. Klicken Sie mit der rechten Maustaste auf die zu ändernde Richtlinie und klicken Sie dann auf **Eigenschaften**.
2. Geben Sie im Feld **Richtlinienbereich - Minimum** die niedrigste Zahl der fehlgeschlagenen Authentifizierungsversuche an, die von einem Benutzer in dieser Gruppe vorgenommen werden können, bevor das Gerät gesperrt wird.



Hinweis

Die Mindest- und Höchstwerte für den Richtlinienbereich können dem übergeordneten Bereich entsprechen oder geändert werden. Die Mindest- und Höchstwerte können nicht erweitert werden.

3. Geben Sie im Feld **Richtlinienbereich - Maximum** die höchste Zahl der Authentifizierungsversuche an, die von einem Benutzer in dieser Gruppe vorgenommen werden können, bevor die Authentifizierung fehlschläft und das Gerät gesperrt wird.
4. Geben Sie im Feld **Richtlinienwert** die Zahl der fehlgeschlagenen Authentifizierungsversuche an, die von einem Benutzer in dieser Gruppe vorgenommen werden können, bevor das Gerät gesperrt wird.
5. Klicken Sie auf **OK**, um alle in diesem Fenster vorgenommenen Änderungen zu speichern.

   Die Richtlinienänderung wird aktiviert, wenn der Endpunkt-Client mit PolicyServer synchronisiert wird.

Richtlinien mit den Antworten "Wahr/Falsch" oder "Ja/Nein"

Einige Richtlinien weisen nur die Option "Wahr/Falsch" oder "Ja/Nein" auf. Für dieses Beispiel wird **Preboot-Umgehung** verwendet.

Ein Gruppenadministrator kann festlegen, ob Full Disk Encryption Preboot angezeigt wird. Wenn die übergeordnete Gruppe "Ja" und "Nein" zulässt, sind die die Authentifikatoren der Untergruppe berechtigt, den Bereich auf "Ja" und "Nein", nur

"Ja" oder nur "Nein" festzulegen. Wenn für die übergeordnete Gruppe der Bereich auf entweder "Ja" oder "Nein" festgelegt ist, kann der Administrator der Untergruppe nur denselben Bereich auswählen.

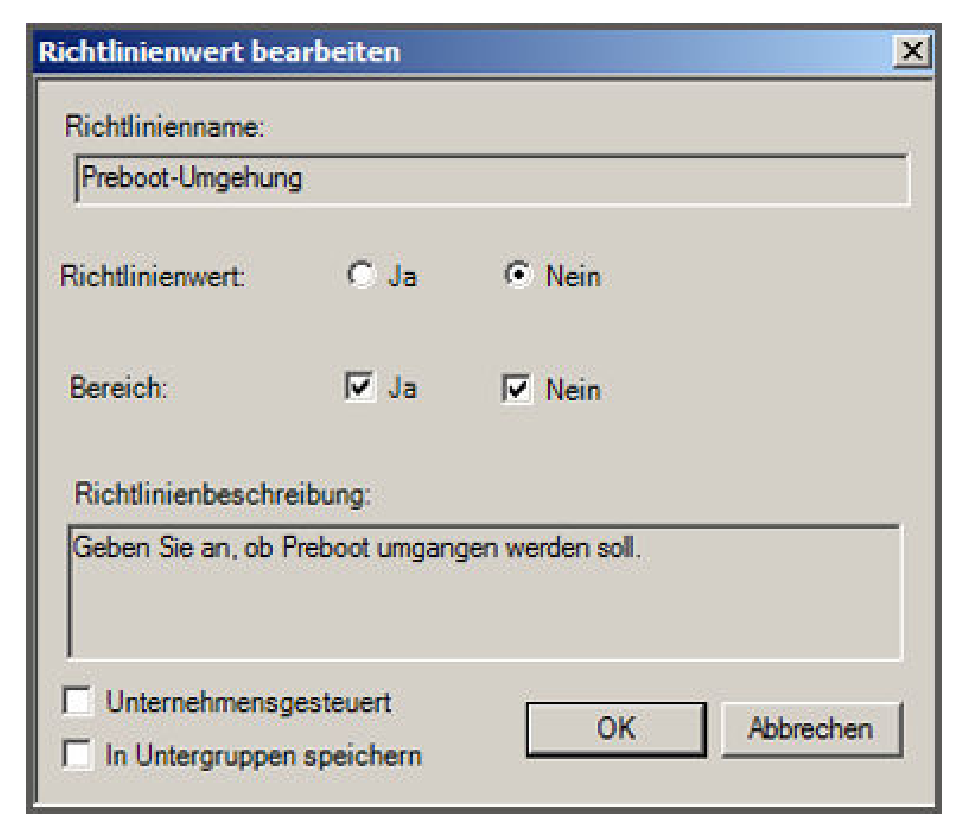


ABBILDUNG 3-3. Richtlinie mit den Werten "Ja/Nein"

Prozedur

1. Klicken Sie mit der rechten Maustaste auf die zu ändernde Richtlinie und klicken Sie dann auf **Eigenschaften**.

2. Mit dem Feld **Richtlinienwert** wird festgelegt, ob die Richtlinie aktiviert wird.

3. Mit dem Feld **Bereich** wird festgelegt, ob diese Richtlinie anderen Benutzern oder Gruppen zur Verfügung steht. Wenn diese Richtlinie beispielsweise von einem Enterprise Administrator in Enterprise Richtlinien auf **Nein** festgelegt wurde, kann die Richtlinie nicht von anderen Gruppen auf "Yes" festgelegt werden.

4. Klicken Sie auf **OK**, um alle in diesem Fenster vorgenommenen Änderungen zu speichern.

   Die Richtlinienänderung wird aktiviert, wenn der Endpunkt-Client mit PolicyServer synchronisiert wird.

Richtlinien mit Mehrfach-/Einfachauswahl bearbeiten

Einige Richtlinien verfügen über mehrere Optionen. Die Richtlinie **Aktion zur Gerätesperrung** wird in einem Mehrfach-/Einfachauswahlfenster bearbeitet. Administratoren können nur einen **Richtlinienwert** auswählen. In diesem Beispiel muss

der Gruppenadministrator die durchzuführende Aktion auswählen, wenn ein Benutzer die zulässige Anzahl an Authentifizierungsversuchen überschreitet.

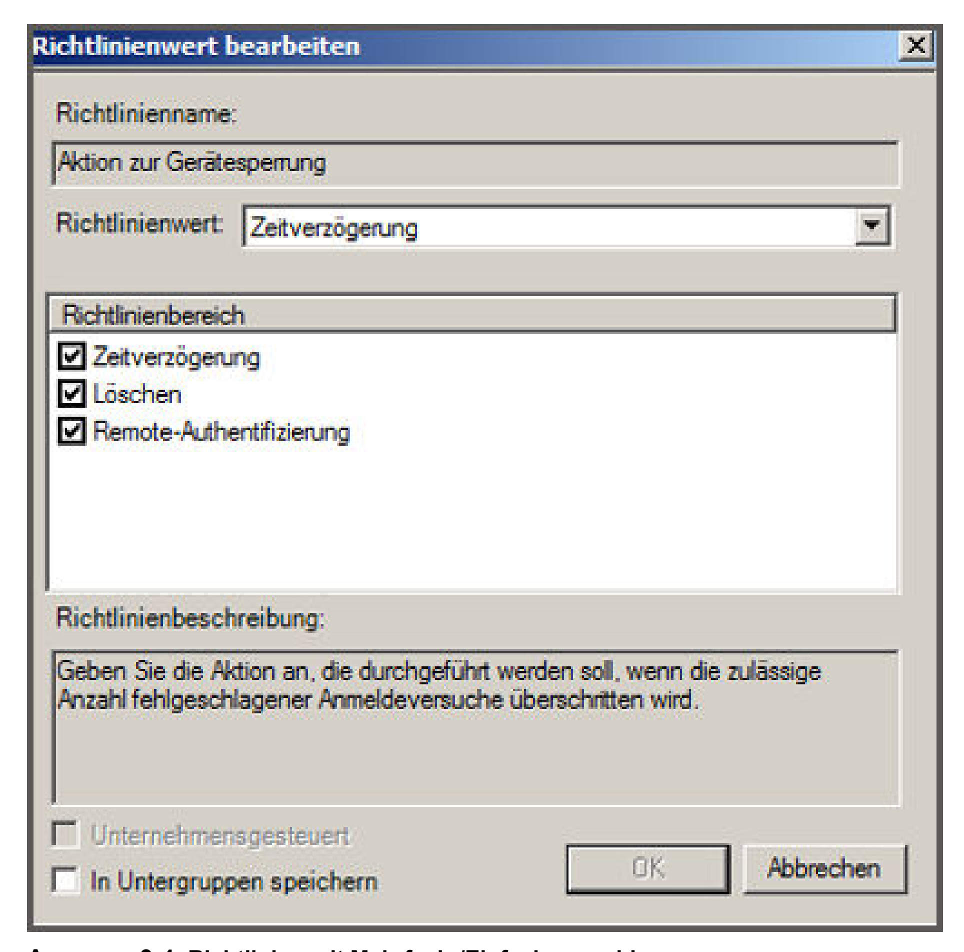


ABBILDUNG 3-4. Richtlinien mit Mehrfach-/Einfachauswahl

Prozedur

1. Klicken Sie mit der rechten Maustaste auf die zu ändernde Richtlinie und klicken Sie dann auf **Eigenschaften**.

2. Wählen Sie die gewünschte Standardeinstellung für das Dropdown-Menü **Richtlinienwert** aus.

3. Wählen Sie die verfügbaren Optionen für den Bereich **Richtlinienbereich** aus.



Hinweis

Durch das Entfernen einer Option wird der Wert aus der Dropdown-Liste **Richtlinienwert** entfernt.

4. Klicken Sie zum Speichern der Änderungen auf **OK**.

   Die Richtlinienänderung wird aktiviert, wenn der Endpunkt-Client mit PolicyServer synchronisiert wird.

Richtlinien mit Textzeichenfolgenargumenten bearbeiten

Einige Richtlinien weisen eine editierbare Textzeichenfolge für einzelne Array-Argumente auf. Die Richtlinie **Kennwort zur Auslöschung** ist ein Beispiel einer Richtlinie, die die Funktion zur Angabe einer Textzeichenfolge bietet.

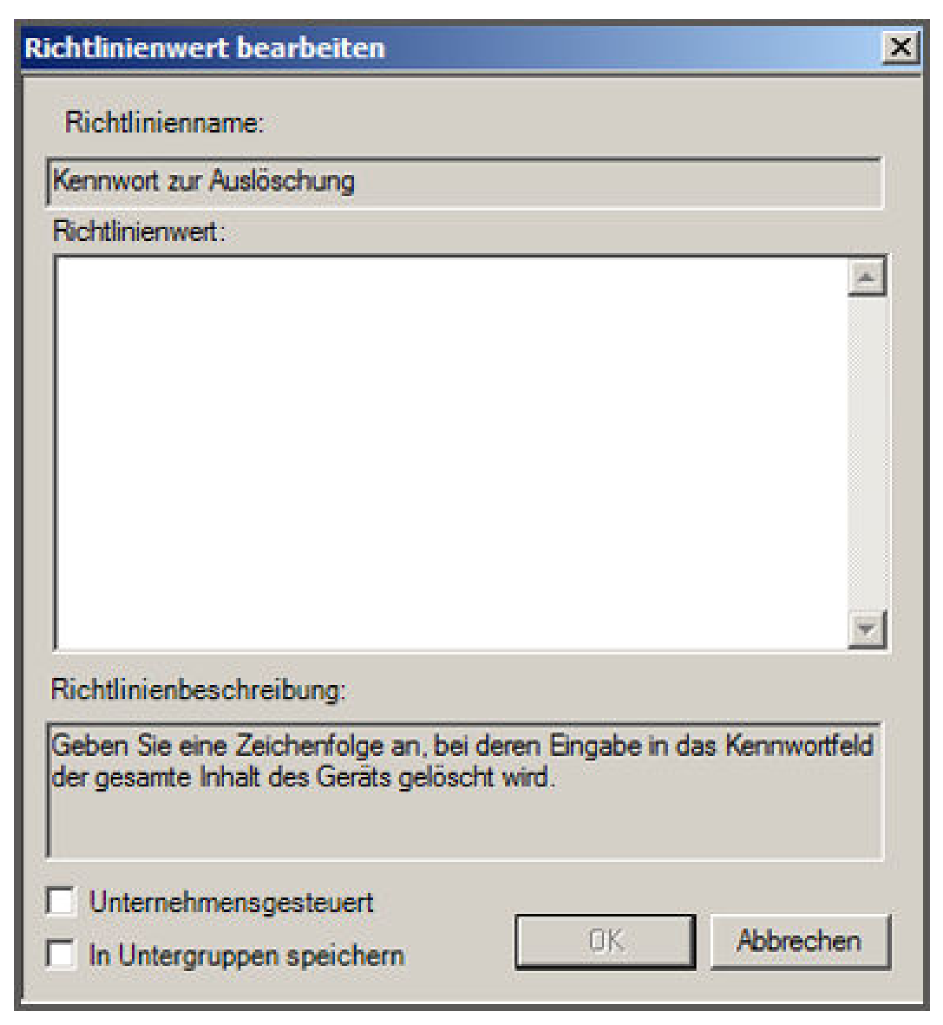


ABBILDUNG 3-5. Richtlinie mit Textzeichenfolgenargument

Prozedur

1. Klicken Sie mit der rechten Maustaste auf die zu ändernde Richtlinie und klicken Sie dann auf **Eigenschaften**.
2. Geben Sie für das Feld **Richtlinienwert** die Abfolge der Zeichen für diese Richtlinie an.
3. Klicken Sie auf **OK**, um alle in diesem Fenster vorgenommenen Änderungen zu speichern.

   Die Richtlinienänderung wird aktiviert, wenn der Endpunkt-Client mit PolicyServer synchronisiert wird.

Richtlinien mit mehreren Optionen bearbeiten

Einige Richtlinien können über mehrere in Unterrichtlinien gespeicherten Optionen verfügen, die sich auf diese Richtlinie auswirken. Mehrere Optionsrichtlinien erstellen getrennte Zeilen in einer Textzeichenfolge, wobei jede Unterrichtlinie eine neue Zeile in der Zeichenfolge darstellt. Beispiel: Die Richtlinie **Falls gefunden** zeigt an, wie ein gefundenes Gerät zurückgegeben wird. Ein normales Adressformat zeigt den Namen, die Straße sowie Stadt/Bundesland/Postleitzahl in drei getrennten Zeilen an.



Hinweis

Die Anzahl der Unterrichtlinien ist auf die Funktionen der Endpunkt-Anwendung begrenzt, die in der Regel nicht mehr als sechs Textzeilen aufweist.

Prozedur

1. Klicken Sie mit der rechten Maustaste auf die zu ändernde Richtlinie und klicken Sie dann auf **Hinzufügen**.

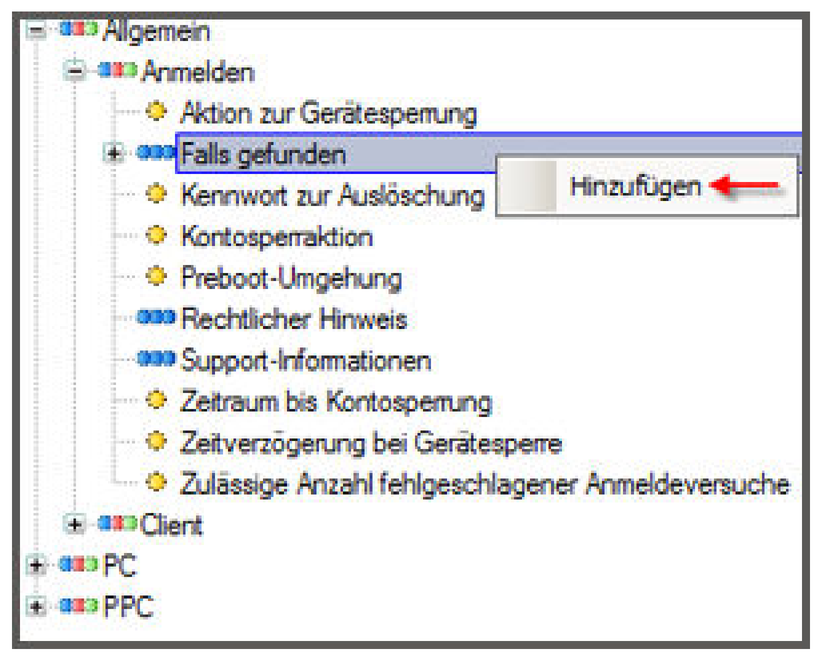


ABBILDUNG 3-6. Falls gefunden-Richtlinie: Neue Option hinzufügen

2. Geben Sie im angezeigten Richtlinienfenster Details im Feld **Richtlinienwert** ein.



Hinweis

Je nach Richtlinie wird möglicherweise eine neue Richtlinie hinzugefügt und anschließend durch Klicken auf die rechte Maustaste und Auswahl von **Eigenschaften** geändert.

---

3. Klicken Sie auf **OK**, um Änderungen in diesem Fenster zu speichern. Wiederholen Sie den Vorgang nach Bedarf.

Falls gefunden	3 Elemente	
Falls gefunden	Name	255 Zeichen
Falls gefunden	Steet Address	255 Zeichen
Falls gefunden	City / State / Zip Code	255 Zeichen

ABBILDUNG 3-7. Falls gefunden-Richtlinie: Ergebnisse nach dem Hinzufügen mehrerer Optionen

4. Um Änderungen vorzunehmen, klicken Sie mit der rechten Maustaste auf die untergeordnete Richtlinie und wählen Sie **Eigenschaften** aus.

   Die Richtlinienänderung wird aktiviert, wenn der Endpunkt-Client mit PolicyServer synchronisiert wird.

PolicyServer Richtlinien

In diesem Abschnitt werden die konfigurierbaren Optionen für alle Unternehmensrichtlinien erläutert, die sich auf PolicyServer auswirken.

Richtlinien für die Admin-Konsole

Richtlinien steuern die Administrations-Tools wie Enterprise Security Manager und PolicyServer MMC.

TABELLE 3-1. PolicyServer Richtlinien für die Admin-Konsole

NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
Zeitüberschreitung der Konsole	Beenden Sie das Administrations-Tool, nachdem das Zeitlimit (in Minuten) ohne Aktivität abgelaufen ist.	1-60 Standard: 20
Zulässige Anzahl fehlgeschlagener Anmeldeversuche	Admin-Anmeldung nach dieser Anzahl aufeinanderfolgender fehlgeschlagener Anmeldeversuche sperren.	0-100 Standard: 0

Name der Richtlinie	Beschreibung	Wertebereich und Standard
Rechtlicher Hinweis	Enthält den rechtlichen Hinweis, der angezeigt werden muss, bevor der Administrator oder Authentifikator die Administrations-Tools verwenden kann.	1-1024 Zeichen Standard: n. v.

Administratorrichtlinien

Richtlinien, die PolicyServer Gruppenadministratorberechtigungen steuern.

Tabelle 3-2. PolicyServer Administratorrichtlinien

Name der Richtlinie	Beschreibung	Wertebereich und Standard
Geräte hinzufügen	Geben Sie an, ob Gruppenadministratoren Geräte hinzufügen dürfen.	Ja, Nein Standard: Ja
Benutzer hinzufügen	Geben Sie an, ob Gruppenadministratoren neue Benutzer hinzufügen dürfen.	Ja, Nein Standard: Ja
Benutzer zu Unternehmen hinzufügen	Geben Sie an, ob Gruppenadministratoren neue Benutzer zum Unternehmen hinzufügen dürfen.	Ja, Nein Standard: Nein
Gruppen hinzufügen/ändern	Geben Sie an, ob Gruppenadministratoren Untergruppen hinzufügen/ändern dürfen.	Ja, Nein Standard: Ja
Richtlinien ändern	Geben Sie an, ob Gruppenadministratoren Richtlinien ändern dürfen.	Ja, Nein Standard: Ja
Gruppen kopieren/einfügen	Geben Sie an, ob Gruppenadministratoren Untergruppen kopieren und einfügen dürfen.	Ja, Nein Standard: Ja
Geräte entfernen	Geben Sie an, ob Gruppenadministratoren Geräte entfernen dürfen.	Ja, Nein Standard: Ja
Gruppen entfernen	Geben Sie an, ob Gruppenadministratoren Untergruppen entfernen dürfen.	Ja, Nein Standard: Ja

Name der Richtlinie	Beschreibung	Wertebereich und Standard
Benutzer entfernen	Geben Sie an, ob Gruppenadministratoren Benutzer entfernen dürfen.	Ja, Nein Standard: Ja
Benutzer von Unternehmen entfernen	Geben Sie an, ob Gruppenadministratoren Benutzer vom Unternehmen entfernen dürfen.	Ja, Nein Standard: Nein

Authentifizierungsrichtlinien

Richtlinien, die Rechte und Berechtigungen von Authentifizierern in Unternehmen regeln.

Tabelle 3-3. PolicyServer Authentifizierungsrichtlinien

Name der Richtlinie	Beschreibung	Wertebereich und Standard
Geräte hinzufügen	Geben Sie an, ob Authentifizierer Geräte hinzufügen dürfen.	Ja, Nein Standard: Nein
Benutzer hinzufügen	Geben Sie an, ob Authentifizierer neue Benutzer hinzufügen dürfen.	Ja, Nein Standard: Nein
Benutzer zu Unternehmen hinzufügen	Geben Sie an, ob Authentifizierer neue Benutzer zum Unternehmen hinzufügen dürfen.	Ja, Nein Standard: Nein
Gruppen hinzufügen/ändern	Geben Sie an, ob Authentifizierer Untergruppen hinzufügen/ändern dürfen.	Ja, Nein Standard: Nein
Gruppen kopieren/ einfügen	Geben Sie an, ob Authentifizierer Untergruppen kopieren und einfügen dürfen.	Ja, Nein Standard: Nein
Geräte entfernen	Geben Sie an, ob Authentifizierer Geräte entfernen dürfen.	Ja, Nein Standard: Nein
Gruppen entfernen	Geben Sie an, ob Authentifizierer Untergruppen entfernen dürfen.	Ja, Nein Standard: Nein

NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
Benutzer entfernen	Geben Sie an, ob Authentifizierer Benutzer entfernen dürfen.	Ja, Nein Standard: Nein
Benutzer von Unternehmen entfernen	Geben Sie an, ob Authentifizierer Benutzer vom Unternehmen entfernen dürfen.	Ja, Nein Standard: Nein

Richtlinien für Protokollwarnungen

Richtlinien, die E-Mail-Nachrichten regeln, die zu wichtigen PolicyServer Protokollereignissen gesendet werden.

TABELLE 3-4. Richtlinien für PolicyServer Protokollwarnungen

NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
E-Mail-Absenderadresse	Geben Sie die E-Mail-Adresse an, die als Quell-E-Mail-Adresse für die Warnungsbenachrichtigungen verwendet wird.	1-255 Zeichen Standard: n. v.
SMTP-Servername	Geben Sie den SMTP-Server an, der für das Senden von E-Mail-Nachrichten mit Warnungen verantwortlich ist.	1-255 Zeichen Standard: n. v.

PDA-Richtlinien

Richtlinien, mit denen festgelegt wird, wie PDA-Geräte mit PolicyServer kommunizieren können.

Tabelle 3-5. PolicyServer PDA-Richtlinien

Kategorie	Name der Richtlinie	Beschreibung	Wertebereich und Standard
PDA	Handy-PDA	Geben Sie an, ob Handy-PDA-Geräte per SMS benachrichtigt werden, oder senden Sie die Installationsnachricht per E-Mail.	SMS, E-Mail, Keine Standard: Keine
PDA	E-Mail	E-Mail-Einstellungen zum Senden von Installationsbenachrichtigungen an den Benutzer.	
PDA > **E-Mail**	SMTP-Servername	Geben Sie den SMTP-Server an, der für das Senden von E-Mail-Nachrichten verantwortlich ist.	1-255 Zeichen
PDA > **E-Mail**	Betreff	Geben Sie den Betrefftext an, der dem Benutzer in der Betreffzeile der E-Mail angezeigt wird.	1-255 Zeichen
PDA	SMS	Geben Sie an, ob Geräte per SMS darüber benachrichtigt werden, wenn sich Richtlinien-/ Benutzereinstellungen geändert haben.	Aktivieren, Deaktivieren Standard: Deaktiviert
PDA > **SMS**	E-Mail-Domäne	Geben Sie die Zieldomäne für die E-Mail an.	1-255 Zeichen
PDA > **SMS**	SMTP-Servername	Geben Sie den SMTP-Server an, der für das Senden der SMS-Benachrichtigungen verantwortlich ist.	1-255 Zeichen
PDA > **SMS**	Quell-E-Mail	Geben Sie die E-Mail-Adresse an, über die die SMS und E-Mail-Benachrichtigungen gesendet wurden.	1-255 Zeichen

KATEGORIE	NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
PDA	Angebundener PDA	Geben Sie an, ob die Installationsnachrichten für Wireless-, Bluetooth- und Handy-PDA-Geräte sowie in ein Cradle eingesetzte Geräte per E-Mail gesendet werden.	E-Mail, Keine Standard: Keine
PDA	Begrüßungsnachricht	Enthält die Datei mit der Begrüßungsnachricht, deren Inhalt dem Benutzer während des Download-Vorgangs angezeigt wird.	1-1024 Zeichen

Richtlinien für das Herunterladen von Service Packs

Richtlinien, mit denen die Zeiten für das automatische Herunterladen von Client-Service Packs gesteuert wird.

TABELLE 3-6. Richtlinien für das Herunterladen von PolicyServer Service Packs

NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
Stunde, zu der das Herunterladen von Service Packs beginnt	Legen Sie die Zeit zum Herunterladen von Service Packs fest.	0-23 Standard: 0
Stunde, zu der das Herunterladen von Service Packs beendet wird	Legen Sie die Zeit fest, zu der das Herunterladen von Service Packs beendet wird.	0-23 Standard: 0

Richtlinien für Begrüßungsnachricht

Richtlinien regeln, ob eine Begrüßungsnachricht an Benutzer gesendet wird, nachdem diese zu einer Gruppe hinzugefügt wurden.

TABELLE 3-7. Richtlinien für PolicyServer Begrüßungsnachricht

NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
Nachricht	Enthält die Datei mit der Begrüßungsnachricht.	1-1024 Zeichen Standard: n. v.
SMTP-Servername	Geben Sie den SMTP-Server an, der für das Senden von Begrüßungsnachrichten per E-Mail verantwortlich ist.	1-255 Zeichen Standard: n. v.
Quell-E-Mail	Geben Sie die E-Mail-Adresse an, die als Quell-E-Mail-Adresse für die Begrüßungsnachricht per E-Mail verwendet wird.	1-255 Zeichen Standard: n. v.
Betreff	Die Betreffzeile der Begrüßungsnachricht.	1-255 Zeichen Standard: n. v.

Richtlinien für Full Disk Encryption

In diesem Abschnitt werden die konfigurierbaren Optionen für alle Richtlinien erläutert, die sich auf Full Disk Encryption-Clients auswirken.

Allgemeine Richtlinien

Allgemeine Richtlinien, die sich auf die Full Disk Encryption auswirken, einschließlich Anmeldung, Deinstallation der Full Disk Encryption sowie Sperren von Geräten.

TABELLE 3-8. Allgemeine Richtlinien für Full Disk Encryption

KATEGORIE	NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
Client	Deinstallation durch Benutzer zulassen	Geben Sie an, ob Full Disk Encryption vom Benutzer deinstalliert werden kann.	Ja, Nein Standard: Nein

Kategorie	Name der Richtlinie	Beschreibung	Wertebereich und Standard
Anmelden	Kontosperraktion	Legen Sie die Aktion fest, die durchgeführt werden soll, wenn das Gerät keine Kommunikation mit dem PolicyServer entsprechend der Festlegung in der Richtlinie "Zeitraum bis Kontosperrung" aufbaut. • Löschen: Der gesamte Inhalt auf dem Gerät wird gelöscht. • Remote-Authentifizierung: Erfordert, dass der Benutzer eine Remote-Authentifizierung durchführt.	Löschen, Remote-Authentifizierung Standard: Remote-Authentifizierung
Anmelden	Zeitraum bis Kontosperrung	Geben Sie die Anzahl der Tage an, die für den Client ohne Kommunikation mit dem PolicyServer zulässig sind.	0-999 Standard: 360
Anmelden	Kennwort zur Auslöschung	Geben Sie eine Zeichenfolge an, bei deren Eingabe der gesamte Inhalt auf dem Gerät gelöscht wird.	1-255 Zeichen Standard: n. v.
Anmelden	Aktion zur Gerätesperrung	Geben Sie die Aktion an, die durchgeführt wird, wenn das Gerät gesperrt wird. • Zeitverzögerung: Der Zeitraum, der vergehen muss, bis der Benutzer sich erneut Anmelden kann. • Löschen: Der gesamte Inhalt auf dem Gerät wird gelöscht. • Remote-Authentifizierung: Erfordert, dass der Benutzer eine Remote-Authentifizierung durchführt.	Zeitverzögerung, Löschen, Remote-Authentifizierung Standard: Zeitverzögerung

Kategorie	Name der Richtlinie	Beschreibung	Wertebereich und Standard
Anmelden	Zulässige Anzahl fehlgeschlagener Anmeldeversuche	Geben Sie die Anzahl der zulässigen fehlgeschlagenen Anmeldeversuche an, bevor die Zeitverzögerung zur Gerätesperre aktiviert wird.	0-100 Standard: 5
Anmeldung > **Falls gefunden**	Falls gefunden	Geben Sie die anzuzeigenden Informationen an.	1-255 Zeichen Standard: n. v.
Anmelden	Rechtlicher Hinweis	Geben Sie an, ob ein rechtlicher Hinweis angezeigt werden soll.	Aktivieren/ Deaktivieren Standard: Deaktiviert
Anmeldung > **Rechtlicher Hinweis**	Anzeigezeit für den rechtlichen Hinweis	Geben Sie an, wann dem Benutzer der rechtliche Hinweis angezeigt werden soll.	Installation, Start Standard: Start
Anmeldung > **Rechtlicher Hinweis**	Text des rechtlichen Hinweises	Geben Sie den Text des rechtlichen Hinweises an.	Datei einfügen Standard: n. v.
Anmelden	Zeitverzögerung bei Gerätesperre	Gerät für X Minuten sperren, wenn der Benutzer die zulässige Anzahl fehlgeschlagener Anmeldeversuche überschreitet.	1-999,999 Standard: 1
Anmelden	Preboot-Umgehung	Geben Sie an, ob Preboot umgangen werden soll.	Ja, Nein Standard: Nein
Anmeldung > **Support-Informationen**	Support-Informationen	Zeigen Sie Informationen zum Helpdesk bzw. den Administratorkontakt an.	Standard: n. v.

PC-Richtlinien

Richtlinien, die Geräte oder Laptops regeln, auf denen Full Disk Encryption ausgeführt wird.

TABELLE 3-9. PC-Richtlinien für Full Disk Encryption

KATEGORIE	NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
Client	Wiederherstellung durch Benutzer zulassen	Geben Sie an, ob Benutzer auf dem Gerät auf Dienstprogramme für die Systemwiederherstellung zugreifen können.	Ja, Nein Standard: Nein
Verschlüsselung	Gerät verschlüsseln	Geben Sie an, ob das Gerät verschlüsselt werden soll.	Ja, Nein Standard: Ja
Anmelden	Token-Authentifizierung	Richtlinie hinsichtlich physischer Token, einschließlich Smartcards und USB-Token. Alle Unterrichtlinien sind nur sichtbar, wenn die Token-Authentifizierung aktiviert ist.	Aktivieren, Deaktivieren Standard: Deaktiviert
Anmeldung > **Token-Authentifizierung**	OCSP-Validierung	Das Verifizieren der Zertifikate über OCSP ermöglicht das Widerrufen ungültiger Zertifikate durch die Zertifizierungsstelle. **Hinweis** Alle Unterrichtlinien sind nur sichtbar, wenn die OCSP-Validierung aktiviert ist.	Aktivieren, Deaktivieren Standard: Deaktiviert
Anmeldung > **Token-Authentifizierung** > **OCSP-Validierung**	OCSP-CA-Zertifikate	Zertifikate der Zertifizierungsstelle.	0-1024 Byte Standard: n. v.

Kategorie	**Name der Richtlinie**	**Beschreibung**	**Wertebereich und Standard**
Anmeldung > **Token-Authentifizierung** > **OCSP-Validierung**	OCSP - Aktion bei Zertifikatsstatus 'Abgelaufen'	Definiert die Aktion, die bei Ablauf des OCSP-Zertifikatsstatus ausgeführt wird.	Zeitverzögerung, Löschen, Remote-Authentifizierung, Anmeldung verweigern, Zugriff zulassen Standard: Anmeldung verweigern
Anmeldung > **Token-Authentifizierung** > **OCSP-Validierung**	OCSP-Übergangsfrist	Eine Übergangsfrist in Tagen, in der die Authentifizierung erfolgen kann, selbst wenn der OCSP-Server das Zertifikat innerhalb dieser Frist nicht verifiziert hat.	0-365 Standard: 7
Anmeldung > **Token-Authentifizierung** > **OCSP-Validierung**	OCSP-Responder	Zertifikate der Zertifizierungsstelle.	Ja, Nein Standard: Ja
Anmeldung > **Token-Authentifizierung** > **OCSP-Validierung** > **OCSP-Responder**	OCSP-Responder-Zertifikat	Zertifikat der Zertifizierungsstelle	0-1024 Byte Standard: n. v.
Anmeldung > **Token-Authentifizierung** > **OCSP-Validierung** > **OCSP-Responder**	OCSP-Responder-URL	Zertifikate der Zertifizierungsstelle.	0-1024 Byte Standard: n. v.

Kategorie	Name der Richtlinie	Beschreibung	Wertebereich und Standard
Anmeldung > **Token-Authentifizierung** > **OCSP-Validierung**	OCSP - Aktion bei Zertifikatsstatus 'Widerrufen'	Definiert die Aktion, die bei Widerruf des OCSP-Zertifikatsstatus ausgeführt wird.	Zeitverzögerung, Löschen, Remote-Authentifizierung, Anmeldung verweigern, Zugriff zulassen Standard: Anmeldung verweigern
Anmeldung > **Token-Authentifizierung** > **OCSP-Validierung**	OCSP - Erfolg anzeigen	Ob der Erfolg der OCSP-Anwort angezeigt werden soll.	Ja, Nein Standard: Ja
Anmeldung > **Token-Authentifizierung** > **OCSP-Validierung**	OCSP - Aktion bei Zertifikatsstatus 'Unbekannt'	Geben Sie die Aktion an, die durchgeführt wird, wenn der OCSP-Zertifikatsstatus 'Unbekannt' lautet.	Zeitverzögerung, Löschen, Remote-Authentifizierung, Anmeldung verweigern, Zugriff zulassen Standard: Anmeldung verweigern
Anmelden	Token-Durchleitung	Das Token wird während des Startvorgangs zur weiteren Verarbeitung an Desktop-GINA übergeben.	Ja, Nein Standard: Nein
Kennwort	Zulässige Authentifizierungsmethoden	Geben Sie die zulässigen Authentifizierungsmethoden an, die verwendet werden können.	Fest, ColorCode, PIN, Remote, RSA Standard: Fest

PPC-Richtlinien

Richtlinien, die Full Disk Encryption für PPC-Pocket-Geräte regeln.

Tabelle 3-10. Richtlinien für Full Disk Encryption von PPC-Geräten

Kategorie	Name der Richtlinie	Beschreibung	Wertebereich und Standard
Verschlüsselung	PPC - Termine verschlüsseln	Geben Sie an, ob die Termindatenbank auf dem PPC-Gerät verschlüsselt werden soll.	Ja, Nein Standard: Ja
Verschlüsselung	PPC - Kontakte verschlüsseln	Geben Sie an, ob die Kontaktdatenbank auf dem PPC-Gerät verschlüsselt werden soll.	Ja, Nein Standard: Ja
Verschlüsselung	PPC - Gerät verschlüsseln	Geben Sie an, ob alle externen Medien und der gesamte interne Speicher auf dem PPC-Gerät verschlüsselt werden sollen.	Ja, Nein Standard: Ja
Verschlüsselung	PPC - E-Mail verschlüsseln	Geben Sie an, ob die E-Mail-Datenbank auf dem PPC-Gerät verschlüsselt werden soll.	Ja, Nein Standard: Ja
Verschlüsselung	PPC - Sonstige Datenbanken verschlüsseln	Geben Sie eine Liste der Datenbanken an, die auf dem PPC-Gerät verschlüsselt werden sollen.	1-255 Zeichen Standard: n. v.
Verschlüsselung > **PPC - Sonstige Datenbanken verschlüsseln**	PPC - Aufgaben verschlüsseln	Geben Sie an, ob die Aufgabendatenbank auf dem PPC-Gerät verschlüsselt werden soll.	Ja, Nein Standard: Ja
PPC	Protokollierung	Richtlinien, die die Protokolldatei auf dem PPC-Gerät definieren.	

KATEGORIE	NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
Protokollierung	Größe der PPC-Protokolldatei	Geben Sie die Größe der Protokolldatei (in KB) auf dem PPC-Gerät an.	5-512 Standard: 512
Anmelden	Notruf zulassen	Geben Sie an, ob die Benutzer Notrufe von ihren Geräten aus vornehmen dürfen.	Ja, Nein Standard: Nein
Anmelden	PPC - Kontosperraktion	Legen Sie die Aktion fest, die durchgeführt werden soll, wenn das Gerät keine Kommunikation mit dem PolicyServer entsprechend der Festlegung in der Richtlinie "Zeitraum bis Kontosperrung" aufbaut. Folgende Aktionen sind möglich: • Löschen: Der gesamte Inhalt auf dem Gerät wird gelöscht. • Remote-Authentifizierung: Erfordert, dass der Benutzer eine Remote-Authentifizierung durchführt.	Löschen, Remote-Authentifizierung Standard: Remote-Authentifizierung
Anmelden	PPC - Zeitlimit für Gerät	Geben Sie die Anzahl der Minuten an, die das Authentifizierungsfenster im inaktiven Zustand angezeigt wird.	0-60 Standard: 1
Anmelden	PPC - Nach Anmeldung starten	Geben Sie eine nach erfolgter Authentifizierung auf dem Gerät zu startende Anwendung an.	1-255 Zeichen Standard: n. v.
Kennwort	PPC - Authentifizierungsmethoden	Geben Sie die auf dem PPC-Gerät zulässigen Authentifizierungsmethoden an.	Fest, ColorCode, PIN, Remote Standard: Fest

KATEGORIE	NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
PPC	PPC - Datenträger bei Wipe löschen	Beim Geräte-Wipe werden die Daten auf gemounteten Datenträgern gelöscht.	Ja, Nein Standard: Nein

FileArmor Richtlinien

In diesem Abschnitt werden die konfigurierbaren Optionen für alle Unternehmensrichtlinien erläutert, die sich auf FileArmor Clients auswirken.

Computerrichtlinien

Richtlinien, die die Installationsberechtigungen auf Geräten regeln, auf denen FileArmor installiert ist.

TABELLE 3-11. FileArmor Computerrichtlinien

KATEGORIE	NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
Computer	Deinstallation durch Benutzer zulassen	Diese Richtlinien gibt an, ob ein anderer Benutzer als der Administrator die Endpunktanwendung deinstallieren kann.	Ja, Nein Standard: Ja

Verschlüsselungsrichtlinien

Richtlinien für die Verarbeitung der Verschlüsselung auf FileArmor Geräten.

TABELLE 3-12. FileArmor Verschlüsselungsrichtlinien

KATEGORIE	NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
	Sicheres Löschen zulassen	Geben Sie an, ob der Benutzer Dateien löschen darf.	Ja, Nein Standard: Ja
	Optisches Laufwerk deaktivieren	Deaktivieren Sie den Zugriff auf CD- bzw. DVD-Laufwerke.	Ja, Nein Standard: Nein
	Verwendeter Verschlüsselungsschlüssel	• Benutzerschlüssel: Wählen Sie einen für den Benutzer eindeutigen Schlüssel aus. • Gruppenschlüssel: Wählen Sie einen für die Gruppe eindeutigen Schlüssel aus, damit auch alle Benutzer in der Gruppe auf die Dateien zugreifen können. • Unternehmensschlüssel: Wählen Sie einen für das Unternehmen eindeutigen Schlüssel aus, damit auch alle Benutzer im Unternehmen auf die Dateien zugreifen können.	Benutzerschlüssel, Gruppenschlüssel, Unternehmensschlüssel Standard: Gruppenschlüssel
	Zulässige Verschlüsselungsmethode	Wählen Sie die zulässigen Methoden zum Verschlüsseln von Dateien aus: 1. Benutzerschlüssel 2. Gruppenschlüssel 3. Benutzerdefiniertes Kennwort 4. Digitale Zertifikate	Eindeutiger Schlüssel des Benutzers, Eindeutiger Schlüssel der Gruppe, Mit statischem Kennwort verschlüsseln, Mit Zertifikat verschlüsseln Standard: Alle

KATEGORIE	NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
Wechselmedien	Gerät vollständig verschlüsseln	Geben Sie an, ob alle Dateien/ Ordner auf den Wechselmedien verschlüsselt werden sollen.	Ja, Nein Standard: Nein
Wechselmedien	USB-Geräte zulassen	Geben Sie die zulässigen USB-Geräte an.	Alle, KeyArmor Standard: Beliebig
Wechselmedien	USB-Laufwerk deaktivieren	Deaktivieren Sie das USB-Laufwerk, wenn es nicht angemeldet ist, deaktivieren Sie es immer oder niemals.	Immer, Abgemeldet, Niemals Standard: Abgemeldet
Wechselmedien	Zu verschlüsselnde Ordner auf Wechselmedien	Der Laufwerksbuchstabe ist vorgegeben und der Richtlinienwert entspricht einem gültigen Wechselmedium. Nicht vorhandene Ordner werden erstellt. Wenn kein Laufwerksbuchstabe angegeben wird, verwenden alle bei der Anmeldung am Gerät angeschlossenen Wechselmedien die Richtlinienwerte.	1-255 Zeichen Standard: n. v.
Wechselmedien	Gerät vollständig verschlüsseln	Geben Sie an, ob alle Dateien/ Ordner auf den Wechselmedien verschlüsselt werden sollen	Ja, Nein Standard: Nein
	Ordner zum Verschlüsseln angeben	Listen Sie die Ordner auf, die auf der Festplatte verschlüsselt werden sollen. Nicht vorhandene Ordner werden erstellt. Außerdem muss auf dem Festplattenlaufwerk ein gültiger Laufwerksbuchstabe bereitgestellt werden. Ein gültiger Richtlinienwert lautet: C:\EncryptedFolder.	1-255 Zeichen Standard: `%DESKTOP%\FileArmor Encrypted`

Anmelderichtlinien

Sicherheitsrichtlinien, die die Anmeldung an FileArmor regeln.

TABELLE 3-13. FileArmor Anmelderichtlinien

KATEGORIE	NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
	Zulässige Authentifizierungsmethoden	Geben Sie die zulässigen Authentifizierungstypen an, die verwendet werden können	Fest, ColorCode, PIN, Smartcard, RSA Standard: Fest
	Aktion zur Gerätesperrung	Die durchzuführende Aktion, wenn das Gerät gesperrt ist.	Zeitverzögerung, Remote-Authentifizierung Standard: Zeitverzögerung
	Zulässige Anzahl fehlgeschlagener Anmeldeversuche	Anzahl der fehlgeschlagenen Anmeldeversuche, bevor die Zeitverzögerung bei Gerätesperre aktiviert wird. 0 ermöglicht eine unbegrenzte Anzahl an Versuchen.	0-100 Standard: 5

Kategorie	Name der Richtlinie	Beschreibung	Wertebereich und Standard
Rechtlicher Hinweis	Anzeigezeit für den rechtlichen Hinweis	Geben Sie an, wann dem Benutzer der rechtliche Hinweis angezeigt wird. **Hinweis** Die Richtlinie ist nur für PolicyServer 3.1.3 (oder neuer) verfügbar und es wird kein rechtlicher Hinweis auf Endpunkten angezeigt, auf denen FileArmor 3.1.3 oder früher ausgeführt wird.	Installation, Start Standard: Start
Rechtlicher Hinweis	Text des rechtlichen Hinweises	Geben Sie den Text des rechtlichen Hinweises an. **Hinweis** Die Richtlinie ist nur für PolicyServer 3.1.3 (oder neuer) verfügbar und es wird kein rechtlicher Hinweis auf Endpunkten angezeigt, auf denen FileArmor 3.1.3 oder früher ausgeführt wird.	Datei einfügen Standard: n. v.
	Zeitverzögerung bei Gerätesperre	Gerät für X Minuten sperren, wenn der Benutzer die zulässige Anzahl fehlgeschlagener Anmeldeversuche überschreitet.	0-999,999 Standard: 1

Kennwortrichtlinien

Richtlinien, die FileArmor Kennwörter regeln.

TABELLE 3-14. FileArmor Kennwortrichtlinien

NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
Kommunikation mit Server erzwingen	Veranlasst FileArmor, nach X Tagen mit dem Server zu kommunizieren. 0 unterdrückt jegliche FileArmor Kommunikation	0-999 Standard: 360
Physischer Token erforderlich	Stellt sicher, dass Benutzer zur Anmeldung einen physischen Token (Smartcards) verwenden.	Ja, Nein Standard: Nein

MobileSentinel Richtlinien

In diesem Abschnitt werden die konfigurierbaren Optionen für MobileSentinel erläutert. Full Disk Encryption verwendet MobileSentinel Richtlinien.

Allgemeine Richtlinien

Richtlinien für alle Geräte, die MobileSentinel verwenden.

TABELLE 3-15. Allgemeine MobileSentinel Richtlinien

KATEGORIE	NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
Allgemein	Einhaltung von Richtlinien	Konformitätsrichtlinien für alle Geräte.	
Allgemein > **Einhaltung von Richtlinien**	Zeitüberschreitung bei Synchronisierung	Geben Sie die Anzahl an Tagen an, während denen ein drahtloses Gerät keine Synchronisierung mit dem PolicyServer durchführen muss. Das Gerät muss zu Synchronisierungszwecken mit dem PolicyServer kommunizieren, wenn die festgelegte Anzahl an Tagen erreicht ist.	0-65.535 Tage Standard: 1

Kategorie	Name der Richtlinie	Beschreibung	Wertebereich und Standard
Allgemein	Netzwerkkonformität	Bestimmen Sie den Zugriff auf die Ressourcen des Unternehmensnetzwerks, indem Sie sicherstellen, dass die Geräte die Unternehmensrichtlinien erfüllen.	
Allgemein > **Netzwerkkonformität**	Adresse für Konformitätsnetzwerk	Geben Sie die IP-Adresse des Netzwerks an, über die das Gerät eine erneute Synchronisierung mit dem PolicyServer durchführen kann, wenn Konformität nicht mehr gewährleistet ist. Wenn bei einem Gerät die Netzwerkkonformität nicht gewährleistet ist, ist dies das einzige Netzwerk, auf das das Gerät zugreifen kann, bis das Gerät wieder konform ist.	1-225 Zeichen Standard: n. v.
Allgemein > **Netzwerkkonformität**	Netzmaske für Konformitätsnetzwerk	Geben Sie die Netzmaske für die Adresse des Konformitätsnetzwerks (Richtlinie "Adresse des Konformitätsnetzwerks") an. Diese Maske und die Adresse dienen dazu, den Zugriff von Geräten auf Netzwerkressourcen außerhalb der eingegebenen Werte zu beschränken, bis das Gerät konform ist.	1-225 Zeichen Standard: n. v.

Kategorie	Name der Richtlinie	Beschreibung	Wertebereich und Standard
Allgemein > **Netzwerkkonformität**	Adresse des Konformitätsservers	Geben Sie die Adresse des PolicyServers an, der als Host für die drahtlosen Geräte in dieser Gruppe verwendet wird. Die Serveradresse für drahtlose Geräte ist der Server, den Geräte kontaktieren, wenn beim Gerät eine Synchronisierungsanforderung eingeht oder wenn das Gerät erkennt, dass eine Synchronisierung mit dem Server notwendig ist, um sicherzustellen, dass die Richtlinien aktualisiert wurden.	1-225 Zeichen Standard: n. v.

PPC-Richtlinien

Spezielle Richtlinien für MobileSentinel PC-Geräte.

Tabelle 3-16. MobileSentinel PPC-Richtlinien

Kategorie	Name der Richtlinie	Beschreibung	Wertebereich und Standard
PPC	Einhaltung von Richtlinien	Spezielle Richtlinien für PPC-Geräte.	
PPC > **Einhaltung von Richtlinien**	PPC - Liste der Konformitätsobjekte	Geben Sie die Objekte an, die auf dem PPC-Gerät benötigt werden. Das Netzwerk-Routing wird auf das Konformitätsnetzwerk begrenzt, wenn sich diese Objekte nicht auf dem Gerät befinden.	Aktivieren, Deaktivieren Standard: Deaktiviert

KATEGORIE	NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
PPC > **PPC - Liste der Konformitätsobjekte**	PPC - Einschränkung auf Konformitätsnetzwerk	Legt fest, ob der Netzwerkzugriff eingeschränkt werden soll, wenn das Gerät nicht konform ist.	Ja, Nein Standard: Ja
PPC > **PPC - Liste der Konformitätsobjekte**	PPC - Automatische Objektwiederherstellung	Legen Sie den Richtlinienwert auf 'Ja' fest, wenn das Objekt, das auf dem Gerät fehlt, automatisch wiederhergestellt werden soll. Legen Sie den Richtlinienwert auf "Nein" fest, um den Benutzer zu der URL-Adresse zu leiten, die in der Richtlinie "PPC - Korrektur-URL" angegeben ist.	
PPC > **PPC - Liste der Konformitätsobjekte** > **PPC - Automatische Objektwiederherstellung**	PPC - Objekt automatisch wiederherstellen	Geben Sie das Objekt an, das auf dem PPC-Gerät wiederhergestellt werden soll, wenn die Richtlinie "PPC - Automatische Objektwiederherstellung" aktiviert wurde.	
PPC > **PPC - Liste der Konformitätsobjekte** > **PPC - Automatische Objektwiederherstellung**	PPC - Objekt automatisch wiederherstellen - Ausführungs-Flag	Geben Sie die Aktionen an, die auf das Korrekturobjekt angewendet werden sollen.	Kopieren, Ausführen Standard: Kopieren
PPC > **PPC - Liste der Konformitätsobjekte**	PPC - Informationen zu Konformitätsobjekten	Geben Sie die Informationen für Benutzer an, wenn das angegebene Objekt nicht konform ist.	1-255 Zeichen Standard: n. v.

Kategorie	Name der Richtlinie	Beschreibung	Wertebereich und Standard
PPC > **PPC - Liste der Konformitätsobjekte**	PPC - Objektname	Geben Sie den vollständig qualifizierten Pfadnamen für das Konformitätsobjekt an.	1-255 Zeichen Standard: n. v.
PPC > **PPC - Liste der Konformitätsobjekte**	PPC - Objektversion	Geben Sie die Mindestversionsnummer für das Konformitätsobjekt an. Wenn dieser Richtlinienwert leer gelassen wird, wird die Objektversion nicht auf Konformität geprüft.	1-255 Zeichen Standard: n. v.
PPC > **PPC - Liste der Konformitätsobjekte**	PPC - Korrektur-URL	Geben Sie die Korrektur-URL-Adresse an, die angezeigt werden soll, wenn die Richtlinie "PPC - Automatische Objektwiederherstellung" auf "falsch" festgelegt ist.	1-255 Zeichen Standard: n. v.
PPC	Geräteverwaltung	Spezielle Richtlinien für das Erfassen von Gerätedaten.	
PPC > **Geräteverwaltung**	Intervall zum Erfassen von Geräteattributen	Wichtige Informationen zur Hardware und Software alle X Tage erfassen: 0 = aus	0-365 Tage Standard: 30
PPC > **Geräteverwaltung**	Intervall zum Erfassen von Verzeichnisinformationen	Snapshot von Dateien und Verzeichnissen alle X Tage durchführen: 0 = aus	0-365 Tage Standard: 7
PPC	Bluetooth deaktivieren	Deaktivieren/Aktivieren Sie die Verwendung der BlueTooth-Funkverbindung.	Ja, Nein Standard: Nein
PPC	PPC - Neue Anwendungen deaktivieren	Deaktivieren/Aktivieren Sie das Hinzufügen neuer Anwendungen über Installationsprogramme für Windows Mobile.	Ja, Nein Standard: Nein

Kategorie	Name der Richtlinie	Beschreibung	Wertebereich und Standard
PPC	PPC - Neue Anwendungen deaktivieren	Deaktivieren/Aktivieren Sie das Hinzufügen neuer Anwendungen über Installationsprogramme für Windows Mobile.	Ja, Nein Standard: Nein
PPC	PPC - OBEX deaktivieren	Deaktivieren/Aktivieren Sie eingehende Anforderungen zum Objektaustausch über IR und BlueTooth.	Ja, Nein Standard: Nein

KeyArmor Richtlinien

In diesem Abschnitt werden die konfigurierbaren Optionen für alle Unternehmensrichtlinien erläutert, mit denen KeyArmor Geräte geregelt werden.

Virenschutzrichtlinien

Sicherheitsrichtlinien für die Steuerung von Virenschutzprogrammen auf KeyArmor Geräten.

Tabelle 3-17. KeyArmor Virenschutzrichtlinien

Name der Richtlinie	Beschreibung	Wertebereich und Standard
Aktion bei infizierter Datei	Gibt an, welche Korrekturaktion durchgeführt wird, wenn eine infizierte Datei gefunden wird.	Datei löschen, Gerät auslöschen Standard: Datei löschen
Zuerst infizierte Datei reparieren	Gibt an, ob versucht werden soll, gefundene infizierte Dateien zu reparieren, bevor die in der Richtlinie "Aktion bei infizierter Datei" vorgeschriebene Aktion durchgeführt wird.	Ja, Nein Standard: Ja

Name der Richtlinie	Beschreibung	Wertebereich und Standard
Update-Intervall	Legt das Update-Intervall für den Virenschutz in Stunden fest. Der Wert 0 bedeutet, dass niemals Updates angefordert werden.	0 - 9.999 Stunden Standard: 1
Update-Adresse	Eine Liste mit Server-URLs der Hersteller, die zwecks Updates kontaktiert werden können. Wenn die Liste leer ist, wird der in der Anwendung definierte Standardstandort verwendet.	1 - 255 Zeichen Standard: n. v.

KeyArmor Sicherheitsrichtlinien

Sicherheitsrichtlinien zum Steuern von KeyArmor.

Tabelle 3-18. KeyArmor Richtlinien

Name der Richtlinie	Beschreibung	Wertebereich und Standard
Kennwort zur Auslöschung	Geben Sie eine Zeichenfolge an, bei deren Eingabe der gesamte Inhalt auf dem Gerät gelöscht wird.	1 - 255 Zeichen Standard: n. v.
Zeitüberschreitung bei Inaktivität	Wenn nicht innerhalb von X Minuten auf das KeyArmor Gerät zugegriffen wird, erfolgt eine Abmeldung vom Gerät.	1 - 999 Standard: 15

Anmelderichtlinien

Sicherheitsrichtlinien, die die Anmeldung an KeyArmor regeln.

Tabelle 3-19. KeyArmor Anmelderichtlinien

Name der Richtlinie	Beschreibung	Wertebereich und Standard
Nur einen Benutzer pro Gerät zulassen	In dieser Richtlinie wird festgelegt, ob ein einzelner oder mehrere Benutzer auf ein Gerät zugreifen dürfen. Der Richtlinienwert "Ja" schreibt vor, dass nur ein Benutzer zu einer bestimmten Zeit auf das Gerät zugreifen darf. **Hinweis** Diese Richtlinie wirkt sich nicht auf Administrator- bzw. Authentifiziererrollen aus.	Ja, Nein Standard: Nein
Zulässige Authentifizierungsmethoden	Geben Sie die zulässigen Authentifizierungstypen an, die verwendet werden können.	Fest, ColorCode, PIN, Smartcard, RSA Standard: Fest
Aktion zur Gerätesperrung	Legen Sie die Aktion fest, die durchgeführt werden soll, wenn das Gerät keine Kommunikation mit dem PolicyServer entsprechend der Festlegung in der Richtlinie "Zeitverzögerung bei Gerätesperre" aufbaut.	Löschen, Remote-Authentifizierung, Zeitverzögerung Standard: Remote-Authentifizierung
Zulässige Anzahl fehlgeschlagener Anmeldeversuche	Anzahl der fehlgeschlagenen Anmeldeversuche, bevor die Zeitverzögerung bei Gerätesperre aktiviert wird. 0 ermöglicht eine unbegrenzte Anzahl an Versuchen.	0 - 100 Standard: 5
Zeitverzögerung bei Gerätesperre	Gerät für X Minuten sperren, wenn der Benutzer die zulässige Anzahl fehlgeschlagener Anmeldeversuche überschreitet.	1 -999,999 Standard: 5

Name der Richtlinie	Beschreibung	Wertebereich und Standard
Kennwortsynchronisierung	Diese Richtlinie gibt an, ob Benutzer einer Gruppe ein Kennwort einrichten und es auf anderen Geräten verwenden können, ohne sich über ein Einmalkennwort registrieren zu müssen. Diese Richtlinie wirkt sich nur auf Kennwort des Typs "Fest", "PIN" "ColorCode" und "Zertifikat" aus. Kennwortschemata anderer Hersteller, wie z. B. Microsoft Windows Domänenkennwörter und RSA SecurID, sind nicht betroffen.	Ja, Nein Standard: Nein

Richtlinien für Hinweismeldungen

Meldungen, die Benutzern von KeyArmor Geräten angezeigt werden.

Tabelle 3-20. Richtlinien für KeyArmor Hinweismeldungen

Name der Richtlinie	Beschreibung	Wertebereich und Standard
Falls gefunden	Geben Sie die auf dem Gerät anzuzeigenden Informationen während der Gerätesperre an.	1 - 4096 Zeichen Standard: n. v.
Rechtlicher Hinweis	Rechtliche Hinweise, die dem Benutzer angezeigt werden.	Eingefügte Datei mit 1 - 255 Zeichen Standard: n. v.
Beim Anschließen rechtlichen Hinweis anzeigen	Geben Sie an, ob dem Benutzer als erster Bildschirm ein Hinweis angezeigt werden soll, wenn das KeyArmor Gerät an ein Gerät angeschlossen wird.	Ja, Nein Standard: Nein
Support-Informationen	Zeigen Sie Informationen zum Helpdesk bzw. zum Administratorkontakt an.	1 - 4096 Zeichen Standard: n. v.

PolicyServer Verbindungsrichtlinien

Richtlinien für die Verbindung mit PolicyServer über KeyArmor Geräte.

Tabelle 3-21. PolicyServer Verbindungsrichtlinien

Name der Richtlinie	Beschreibung	Wertebereich und Standard
Aktion, wenn kein Kontakt	Auszuführende Aktion, wenn das KeyArmor Gerät innerhalb des von der Richtlinie "Offline-Zeit bis zum Erzwingen der Verbindung" festgelegten Zeitraums keine Verbindung zum PolicyServer herstellt.	Zeitverzögerung, Remote-Authentifizierung, Wipe Standard: Remote-Authentifizierung
Muss mit PolicyServer verbunden sein	Benutzer zwingen, Verbindung zu PolicyServer herzustellen, um auf Dateien auf dem USB-Gerät zugreifen zu können.	Ja, Nein Standard: Nein
Offline-Zeit bis zum Erzwingen der Verbindung	Der Zeitbedarf in Tagen, bevor ein Benutzer eine Verbindung zum PolicyServer herstellen muss. 0 bedeutet, dass das KeyArmor Gerät keine Verbindung zu PolicyServer herstellen muss.	0 - 999 Standard: 360
Sekundäre Aktion, wenn kein Kontakt	Auszuführende Aktion, wenn das KeyArmor Gerät keine Authentifizierung mit dem PolicyServer durchgeführt hat und der Zeitraum bis zur sekundären Aktion bereits verstrichen ist.	Wipe, Remote-Authentifizierung, Keine Standard: Keine
Zeitraum bis zur sekundären Aktion	Zeitraum in Anzahl Tagen, bis die sekundäre Aktion durchgeführt wird.	0 - 999 Standard: 0

DriveArmor Richtlinien

In diesem Abschnitt werden die konfigurierbaren Optionen für alle Unternehmensrichtlinien erläutert, die sich auf Full Disk Encryption Clients auswirken.



Wichtig

DriveArmor Richtlinien stehen nur dann in PolicyServer 3.1.3 zur Verfügung, wenn PolicyServer von einer früheren Version mit konfigurierten DriveArmor Richtlinien aktualisiert wurde.

Authentifizierungsrichtlinien

Richtlinien für die Authentifizierung auf DriveArmor Geräten.

TABELLE 3-22. Richtlinien für die DriveArmor Authentifizierung

KATEGORIE	NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
Lokale Anmeldung	Zulässige Authentifizierungsmethoden	Geben Sie die zulässigen Authentifizierungsmethoden an, die verwendet werden können.	Fest, Colorcode, PIN Standard: Alle
Lokale Anmeldung	Aktion zur Gerätesperrung	Geben Sie die Aktion an, die durchgeführt wird, wenn das Gerät gesperrt wird. Folgende Aktionen sind möglich: • Löschen: Der gesamte Inhalt auf dem Gerät wird gelöscht. • Remote-Authentifizierung: erfordert, dass der Benutzer eine Remote-Authentifizierung durchführt. • Zeitverzögerung: die Richtlinienaktion "Zeitverzögerung bei Gerätesperre" durchführen.	Zeitverzögerung, Löschen, Remote-Authentifizierung Standard: Zeitverzögerung
Lokale Anmeldung	Zulässige Anzahl fehlgeschlagener Versuche	Geben Sie die Anzahl der zulässigen fehlgeschlagenen Anmeldeversuche an, bevor die Zeitverzögerung bei Gerätesperre aktiviert wird.	0-255 Standard: 10

Kategorie	Name der Richtlinie	Beschreibung	Wertebereich und Standard
Lokale Anmeldung	Zeitverzögerung bei Gerätesperre	Gerät für X Minuten sperren, wenn der Benutzer die Richtlinienregel "Zulässige Anzahl fehlgeschlagener Versuche" überschreitet.	1-1000000 Standard: 1
Authentifizierung	Netzwerkanmeldung	Geben Sie Richtlinien bezüglich der Authentifizierung für das Gerät an, auf dem sich das Netzwerk unter Umständen befindet.	
Netzwerkanmeldung	RSA-Authentifizierung	Geben Sie an, ob Benutzer anhand eines RSA ACE-Servers mit Hilfe von SecurID überprüft werden.	Ja, Nein Standard: Nein
Authentifizierung	Token-Authentifizierung	Das Verifizieren der Zertifikate über OCSP ermöglicht das Widerrufen ungültiger Zertifikate durch die Zertifizierungsstelle. Unterrichtlinien werden nur angezeigt, wenn diese Richtlinie aktiviert ist.	Ja, Nein Standard: n. v.
Token-Authentifizierung	OCSP-Validierung	Das Verifizieren der Zertifikate über OCSP ermöglicht das Widerrufen ungültiger Zertifikate durch die Zertifizierungsstelle. Unterrichtlinien werden nur angezeigt, wenn diese Richtlinie aktiviert ist.	Ja, Nein Standard: n. v.
Token-Authentifizierung > **OCSP-Validierung**	OCSP-CA-Zertifikate	Zertifikate der Zertifizierungsstelle.	0-1024 Standard: n. v.

Kategorie	Name der Richtlinie	Beschreibung	Wertebereich und Standard
Token-Authentifizierung > **OCSP-Validierung**	OCSP-Responder	Zertifikate der Zertifizierungsstelle.	Ja, Nein Standard: Ja
OCSP-Validierung > **OCSP-Responder**	OCSP-Responder-Zertifikat	Zertifikate der Zertifizierungsstelle.	0-1024 Standard: n. v.
OCSP-Validierung > **OCSP-Responder**	OCSP-Responder-URL	Zertifikate der Zertifizierungsstelle.	0- 1024 Standard: n. v.
Token-Authentifizierung	Token-Durchleitung	Das Token wird während des Startvorgangs zur weiteren Verarbeitung an Desktop-GINA übergeben.	Ja, Nein Standard: Nein


Hinweis

OCSP ist die Abkürzung von Online Certificate Status Protocol.

Kommunikationsrichtlinien

Geben Sie die Richtlinien an, die die DriveArmor Kommunikation und Informationen regeln.

TABELLE 3-23. DriveArmor Kommunikationsrichtlinien

KATEGORIE	NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
Kommunikation	Kontosperrakti on	Legen Sie die Aktion fest, die durchgeführt werden soll, wenn das Gerät keine Kommunikation mit dem PolicyServer entsprechend der Festlegung in der Richtlinie "Zeitraum bis Kontosperrung" aufbaut. • Löschen: der gesamte Inhalt auf dem Laufwerk wird gelöscht • Remote-Authentifizierung: erfordert, dass der Benutzer eine Remote-Authentifizierung durchführt • Ignorieren: es wird keine Aktion durchgeführt	Löschen, Remote-Authentifizierun g, Ignorieren Standard: Ignorieren
Kommunikation	Zeitraum bis Kontosperrung	Geben Sie die Anzahl der Tage an, die für den Client ohne Kommunikation mit dem PolicyServer zulässig sind.	0-1000000 Standard: 360
Kommunikation	Informationen	Geben Sie die Richtlinien an, die dem Benutzer Informationen bereitstellen.	
Informationen	Falls gefunden	Geben Sie die auf dem Gerät anzuzeigenden Informationen während der Gerätesperre an.	1-1024 Zeichen Standard: n. v.
Informationen	Rechtlicher Hinweis	Geben Sie an, ob ein rechtlicher Hinweis angezeigt werden soll.	

Kategorie	Name der Richtlinie	Beschreibung	Wertebereich und Standard
Anmeldung > **Rechtlicher Hinweis**	Anzeigezeit für den rechtlichen Hinweis	Geben Sie an, wann dem Benutzer der rechtliche Hinweis angezeigt werden soll.	Installation, Start Standard: Start
Anmeldung > **Rechtlicher Hinweis**	Text des rechtlichen Hinweises	Geben Sie den Text des rechtlichen Hinweises an.	Datei einfügen Standard: n. v.
Informationen	Support-Informationen	Zeigen Sie Informationen zum Helpdesk bzw. zum Administratorkontakt an.	1-1024 Zeichen Standard: n. v.
Kommunikation	Synchronisierungsintervall	Geben Sie an, wie oft (in Minuten) DriveArmor versucht, mit dem PolicyServer zu kommunizieren, um aktualisierte Informationen zu erhalten.	0-1000000 Standard: 120

Geräterichtlinien

Geben Sie Richtlinien an, die allgemeine Aktionen auf dem Gerät regeln, auf dem DriveArmor installiert ist.

Tabelle 3-24. DriveArmor Geräterichtlinien

Name der Richtlinie	Beschreibung	Wertebereich und Standard
Benutzern Administratorzugriff gewähren	Geben Sie an, ob Benutzer auf dem Gerät auf Dienstprogramme für die Systemadministration zugreifen können.	Ja, Nein Standard: Nein
Deinstallation durch Benutzer zulassen	Geben Sie an, ob ein standardmäßiger DriveArmor Benutzer DriveArmor deinstallieren kann.	Ja, Nein Standard: Nein

NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
Kennwort zur Auslöschung	Geben Sie eine Zeichenfolge an, bei deren Eingabe das Gerät zerstört wird.	1-255 Zeichen Standard: n. v.
Preboot-Umgehung	Geben Sie an, ob Preboot umgangen werden soll.	Ja, Nein Standard: Nein

Allgemeine Richtlinien

In diesem Abschnitt werden die konfigurierbaren Optionen für alle Unternehmensrichtlinien erläutert, die sich auf alle Endpoint Encryption-Produkte auswirken.

Agent-Richtlinie

TABELLE 3-25. Allgemeine Agent-Richtlinien

NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
Synchronisierungsintervall	Geben Sie an, wie oft (in Minuten) die Anwendung mit PolicyServer kommuniziert, um aktualisierte Informationen zu erhalten.	1-1440 Standard: 30

Authentifizierungsrichtlinien

Geben Sie Richtlinien an, die die Authentifizierung auf Geräten von allen Endpoint Encryption Anwendungen aus regeln.

Tabelle 3-26. Allgemeine Authentifizierungsrichtlinien

Kategorie	Name der Richtlinie	Beschreibung	Wertebereich und Standard
Lokale Anmeldung	Admin-Kennwort	Geben Sie Richtlinien zur ausschließlichen lokalen Authentifizierung am Gerät an.	
Lokale Anmeldung > **Admin-Kennwort**	Zulässige Zeichentypen	Geben Sie an, ob Kennwörter alphanumerische Zeichen, Ziffern, Sonderzeichen oder eine Kombination dieser enthalten dürfen.	Buchstaben, Zahlen und Sonderzeichen Standard: Alle
Lokale Anmeldung > **Admin-Kennwort**	Kann Benutzernamen enthalten	Geben Sie an, ob der Benutzername im Kennwort enthalten sein darf.	Ja, Nein Standard: Ja
Lokale Anmeldung > **Admin-Kennwort**	Zulässige aufeinanderfolgende Zeichen	Geben Sie die Anzahl der zulässigen aufeinanderfolgenden Zeichen in einem Kennwort an.	0-255 Standard: 3
Lokale Anmeldung > **Admin-Kennwort**	Mindestlänge	Geben Sie die zulässige Mindestlänge für Kennwörter an.	0-255 Standard: 6
Lokale Anmeldung > **Admin-Kennwort**	Aufbewahrung des Kennwortverlaufs	Geben Sie die Anzahl der vorherigen Kennwörter an, die der Benutzer nicht verwenden darf.	0-255 Standard: 0
Lokale Anmeldung > **Admin-Kennwort**	Erforderliche Anzahl an Zeichen	Geben Sie die Anzahl an Buchstaben an, die ein Kennwort enthalten muss.	0-255 Standard: 0
Lokale Anmeldung > **Admin-Kennwort**	Erforderliche Anzahl an Kleinbuchstaben	Geben Sie die Anzahl an Kleinbuchstaben an, die ein Kennwort enthalten muss.	0-255 Standard: 0

Kategorie	Name der Richtlinie	Beschreibung	Wertebereich und Standard
Lokale Anmeldung > **Admin-Kennwort**	Erforderliche Anzahl an Ziffern	Geben Sie die Anzahl an numerischen Zeichen an, die ein Kennwort enthalten muss.	0-255 Standard: 0
Lokale Anmeldung > **Admin-Kennwort**	Erforderliche Anzahl an Sonderzeichen	Geben Sie die Anzahl an Sonderzeichen an, die ein Kennwort enthalten muss.	0-255 Standard: 0
Lokale Anmeldung > **Admin-Kennwort**	Erforderliche Anzahl an Großbuchstaben	Geben Sie die Anzahl an Großbuchstaben an, die ein Kennwort enthalten muss.	0-255 Standard: 0
Lokale Anmeldung	Selbsthilfe	Geben Sie die Richtlinien für die Selbsthilfe an.	
Lokale Anmeldung > **Selbsthilfe**	Anzahl der Fragen	Geben Sie die Anzahl der Fragen an, die korrekt beantwortet werden müssen, um den Benutzer zu authentifizieren.	1-6 Standard: 1
Lokale Anmeldung > **Selbsthilfe**	Persönliche Herausforderung	Geben Sie die persönliche(n) Herausforderungsfrage(n) für die Selbsthilfe an.	1-1024 Standard: n. v.
Lokale Anmeldung	Benutzerkennwort	Geben Sie die Richtlinien an, die für Benutzerkennwörter verwendet werden.	
Lokale Anmeldung > **Benutzerkennwort**	Offline-Änderung von Kennwörtern zulassen	Geben Sie an, ob Benutzer ihr Kennwort ändern können, wenn sie nicht mit PolicyServer verbunden sind.	Ja, Nein Standard: Nein

Kategorie	Name der Richtlinie	Beschreibung	Wertebereich und Standard
Lokale Anmeldung > **Benutzerkennwort**	Zulässige Zeichentypen	Geben Sie an, ob Kennwörter alphanumerische Zeichen, Ziffern, Sonderzeichen oder eine Kombination dieser enthalten dürfen.	Buchstaben, Zahlen und Sonderzeichen Standard: Alle
Lokale Anmeldung > **Benutzerkennwort**	Kann Benutzernamen enthalten	Geben Sie an, ob der Benutzername im Kennwort enthalten sein darf.	Ja, Nein Standard: Ja
Lokale Anmeldung > **Benutzerkennwort**	Kennwort ändern alle	Geben Sie (in Tagen) an, wann ein Benutzer sein Kennwort ändern muss.	1-1000000 Standard: 60
Lokale Anmeldung > **Benutzerkennwort**	Zulässige aufeinanderfolgende Zeichen	Geben Sie die Anzahl der zulässigen aufeinanderfolgenden Zeichen in einem Kennwort an.	0-255 Standard: 3
Lokale Anmeldung > **Benutzerkennwort**	Mindestlänge	Geben Sie die zulässige Mindestlänge für Kennwörter an.	0-255 Standard: 6
Lokale Anmeldung > **Benutzerkennwort**	Aufbewahrung des Kennwortverlaufs	Geben Sie die Anzahl der vorherigen Kennwörter an, die der Benutzer nicht verwenden darf.	0-255 Standard: 0
Lokale Anmeldung > **Benutzerkennwort**	Erforderliche Anzahl an Zeichen	Geben Sie die Anzahl an Buchstaben an, die ein Kennwort enthalten muss.	0-255 Standard: 0
Lokale Anmeldung > **Benutzerkennwort**	Erforderliche Anzahl an Kleinbuchstaben	Geben Sie die Anzahl an Kleinbuchstaben an, die ein Kennwort enthalten muss.	0-255 Standard: 0

KATEGORIE	NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
Lokale Anmeldung > **Benutzerkennwort**	Erforderliche Anzahl an Ziffern	Geben Sie die Anzahl an numerischen Zeichen an, die ein Kennwort enthalten muss.	0-255 Standard: 0
Lokale Anmeldung > **Benutzerkennwort**	Erforderliche Anzahl an Sonderzeichen	Geben Sie die Anzahl an Sonderzeichen an, die ein Kennwort enthalten muss.	0-255 Standard: 0
Lokale Anmeldung > **Benutzerkennwort**	Erforderliche Anzahl an Großbuchstaben	Geben Sie die Anzahl an Großbuchstaben an, die ein Kennwort enthalten muss.	0-255 Standard: 0
Lokale Anmeldung > **Benutzerkennwort**	Bei Benutzernamen Schreibung beachten	Geben Sie an, ob im Benutzernamen die Groß- und Kleinschreibung beachtet werden soll.	Ja, Nein Standard: Nein
Netzwerkanmeldung	Eindeutiger Name	Optional: Geben Sie den eindeutigen Namen des Authentifizierungsservers an. Wird kein eindeutiger Name angegeben, wird die Standardnamenskonvention des LDAP-Servers verwendet.	1-255 Standard: n. v.
Netzwerkanmeldung	Domänenauthentifizierung	Gibt an, ob die Windows Anmeldedaten zum Authentifizieren verwendet werden sollen.	Ja, Nein Standard: Nein
Netzwerkanmeldung	Domänenname	NetBIOS-Name der Domäne für Single Sign On. Standard ist der vom PolicyServer verwendete NetBIOS-Wert.	1-255 Standard: n. v.
Netzwerkanmeldung	Host-Name	Geben Sie den Host-Namen an. Der Host-Name kann ein Domänenname sein.	1-255 Standard: n. v.

KATEGORIE	NAME DER RICHTLINIE	BESCHREIBUNG	WERTEBEREICH UND STANDARD
Netzwerkanmeldung	Portnummer	Optional: 0 = Standard verwenden. Gibt den für die Verbindung zu verwendenden Port an. Wenn keine Portnummer angegeben wird, verwendet der LDAP-Anbieter die standardmäßige Portnummer.	0-65535 Standard: 0
Netzwerkanmeldung	Servertyp	Servertyp, der zum Authentifizieren der Anforderungen des Client-Benutzers verwendet wird.	LDAP, LDAProxy Standard: LDAP
Authentifizierung	Benutzer zwischen Anmeldungen speichern	Zuletzt verwendeten Benutzernamen speichern und auf dem Authentifizierungsbildschirm anzeigen.	Ja, Nein Standard: Ja



Kapitel 4

Arbeiten mit Gruppen, Benutzern und Geräten

Endpoint Encryption verwendet sowohl die rollenbasierte als auch die identitätsbasierte Authentifzierung zum Sichern von Daten auf Endpunkten. Durch die ordnungsgemäße Konfiguration von Benutzern, Gruppen und Geräten wird ordnungsgemäß sichergestellt, dass Daten für nicht autorisierte Benutzer verschlüsselt bleiben und das Risiko von Datenverlusten aufgrund versehentlicher Offenlegung oder beabsichtigter Sabotage vermieden werden kann.

Dieses Kapitel umfasst folgende Themen:

- *Arbeiten mit Gruppen auf Seite 4-2*
- *Arbeiten mit Offline-Gruppen auf Seite 4-5*
- *Arbeiten mit Benutzern auf Seite 4-10*
- *Arbeiten mit Kennwörtern auf Seite 4-24*
- *Arbeiten mit Geräten auf Seite 4-32*

Arbeiten mit Gruppen

Gruppen werden in der PolicyServer MMC verwaltet und bestehen aus den folgenden Typen:

TABELLE 4-1. PolicyServer Gruppentypen

GRUPPE	BESCHREIBUNG
Top-Gruppen	Die höchste Stufe der Gruppen im Unternehmen. Jede Top-Gruppe hat einen eindeutigen Knoten unterhalb des Unternehmens.
Untergruppen	Innerhalb einer Top-Gruppe erstellte Gruppen. Eine Untergruppe erbt die Richtlinien ihrer übergeordneten Gruppe. • Richtlinienvererbung findet nur statt, wenn eine Untergruppe erstellt wird. • Richtlinienänderungen an der Gruppe der obersten Ebene werden nicht bis in vorhandene Untergruppen weitergegeben. • Untergruppen-Richtlinien können nicht weniger strenge Einstellungen wie ihre übergeordneten Gruppen aufweisen.



Hinweis

- Untergruppen erben alle vorhandenen Richtlinie der übergeordneten Gruppe. Administratoren müssen Benutzer und Geräte jedoch getrennt hinzufügen.
- Beim Hinzufügen eines Benutzers zu einer Untergruppe wird der Benutzer nicht automatisch zur Top-Gruppe hinzugefügt. Sie können jedoch einen Benutzer sowohl zur Top-Gruppe als auch zur Untergruppe hinzufügen.

Top-Gruppe hinzufügen

Gruppen vereinfachen die Verwaltung von aktivieren Anwendungen, Benutzern, Richtlinien, Untergruppen und Geräten. Die Top-Gruppe ist die Gruppe auf der höchsten Stufe.



Hinweis

Unternehmensadministrator- oder -authentifiziererkonten können nicht zu Gruppen hinzugefügt werden. Um einen Gruppenadministrator zu erstellen, fügen Sie einen Benutzer hinzu und ändern Sie seine Berechtigungen innerhalb der Gruppe.

Prozedur

1. Klicken Sie mit der rechten Maustaste im linken Fenster auf den Namen des Unternehmens und klicken Sie anschließend auf **Top-Gruppe hinzufügen**.

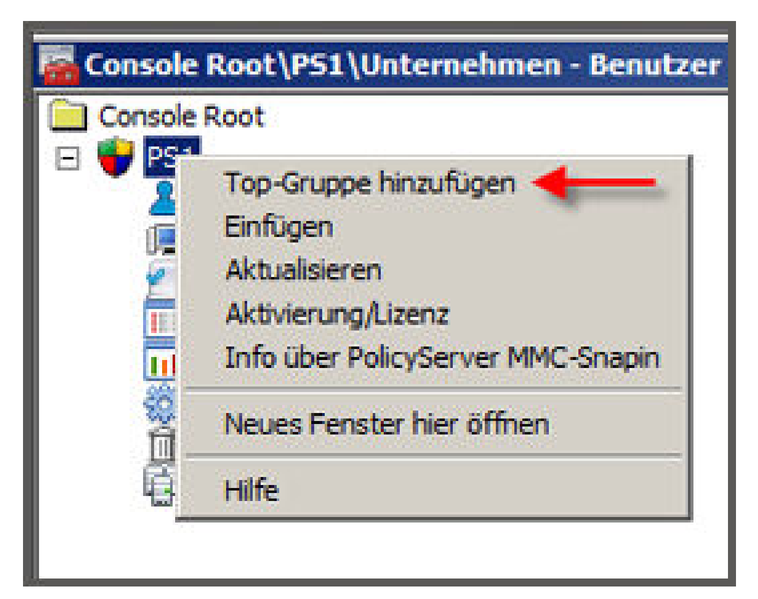


ABBILDUNG 4-1. Top-Gruppe hinzufügen

Das Fenster **Neue Gruppe hinzufügen** wird angezeigt.

2. Geben Sie den Namen und eine Beschreibung der Gruppe an.

3. Wählen Sie **Altgeräte unterstützen** nur aus, wenn Sie Altgeräte verwenden, die die Unicode-Codierung nicht unterstützen. Einige Altgeräte sind möglicherweise nicht in der Lage, unter Verwendung von Unicode mit PolicyServer zu kommunizieren. Weisen verschiedenen Gruppen Unicode und Altgeräte hinzu.

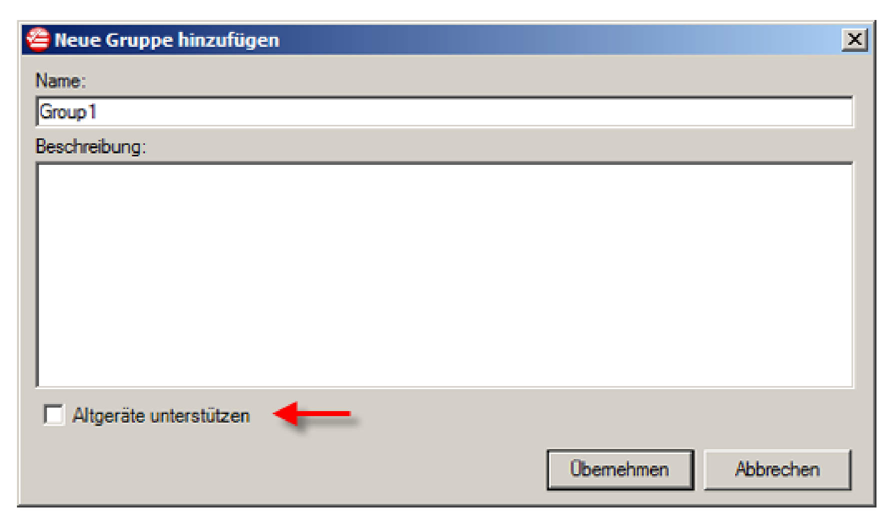


Abbildung 4-2. Neue Gruppe hinzufügen

4. Klicken Sie auf **Übernehmen**.

5. Wenn die Bestätigungsmeldung angezeigt wird, klicken Sie auf **OK**.

   Die neue Gruppe wird zur Baumstruktur im linken Fensterbereich hinzugefügt.

Untergruppe hinzufügen

Untergruppen erben alle vorhandenen Richtlinie der übergeordneten Gruppe. Administratoren müssen Benutzer und Geräte jedoch getrennt hinzufügen.

Prozedur

1. Klicken Sie mit der rechten Maustaste in die linke Fensterstruktur und klicken Sie dann auf **Hinzufügen**.

   Das Fenster **Neue Gruppe hinzufügen** wird angezeigt.

2. Führen Sie die Schritte unter *Top-Gruppe hinzufügen auf Seite 2-6* aus.

Die neue Gruppe wird der Baumstruktur innerhalb der Top-Gruppen-Hierarchie hinzugefügt.

Gruppe ändern

Prozedur

1. Klicken Sie mit der rechten Maustaste in die linke Fensterstruktur und klicken Sie dann auf **Ändern**.

   Das Fenster **Gruppe ändern** wird angezeigt.

2. Geben Sie die Änderungen an und klicken Sie auf **Anwenden**.

Gruppe entfernen

Verwenden Sie die Baumstruktur, um eine Gruppe zu entfernen. Beim Löschen einer Top-Gruppe werden alle Untergruppen ebenfalls entfernt.

Prozedur

1. Klicken Sie mit der rechten Maustaste in die linke Fensterstruktur und klicken Sie dann auf **Entfernen**.

   Die Meldung **PolicyServer Warnung** wird angezeigt.

2. Klicken Sie auf **Ja**, um die Gruppe zu entfernen.

   Die ausgewählte Gruppe wird nicht mehr in der Baumstruktur angezeigt.

Arbeiten mit Offline-Gruppen

Eine Offline-Gruppe ist eine Gruppe von Endpunkt-Clients, die während der Installation keine Verbindung zu PolicyServer herstellen. Die Richtlinien, Benutzer und

Geräte der Gruppe können in eine Datei exportiert und an Offline-Clients weitergeleitet werden. Wenn Änderungen für die Gruppe erforderlich sind, werden diese in eine neue Datei exportiert und erneut an den Offline-Endpunkt-Client gesendet.

Richtlinien werden automatisch aktualisiert, wenn ein Offline-Endpunkt-Client eine Verbindung zu PolicyServer herstellt.



Warnung!

Führen Sie für Full Disk Encryption Clients, die nie eine Verbindung zu PolicyServer herstellen, eine nicht verwaltete Installation aus. Keine Offline-Gruppe ist erforderlich, da Richtlinien mit der Wiederherstellungskonsole verwaltet werden.

Offline-Gruppe erstellen

Gruppen können exportiert werden, um die Installation von Full Disk Encryption und FileArmor auf Geräten zuzulassen, die nicht mit PolicyServer kommunizieren müssen oder können. Die Installationsdateien der Clientanwendung müssen auf dem Server verfügbar sein, auf dem PolicyServer installiert ist.



Hinweis

Exportierte Gruppen müssen mindestens einen Benutzer enthalten. Der Gruppenname muss ebenfalls nur alphanumerisch sein.



Warnung!

Offline-Gruppen können nur für DataArmor SP7 und früher verwendet werden. Führen Sie für Full Disk Encryption Clients, die keine Verbindung zu PolicyServer herstellen, eine nicht verwaltete Installation aus. Richtlinien werden mit der Wiederherstellungskonsole verwaltet.

Prozedur

1. Klicken Sie im linken Fenster mit der rechten Maustaste auf die Gruppe und wählen Sie **Exportieren** aus.

   Der PolicyServer Assistent zum Exportieren von Gruppen wird angezeigt.

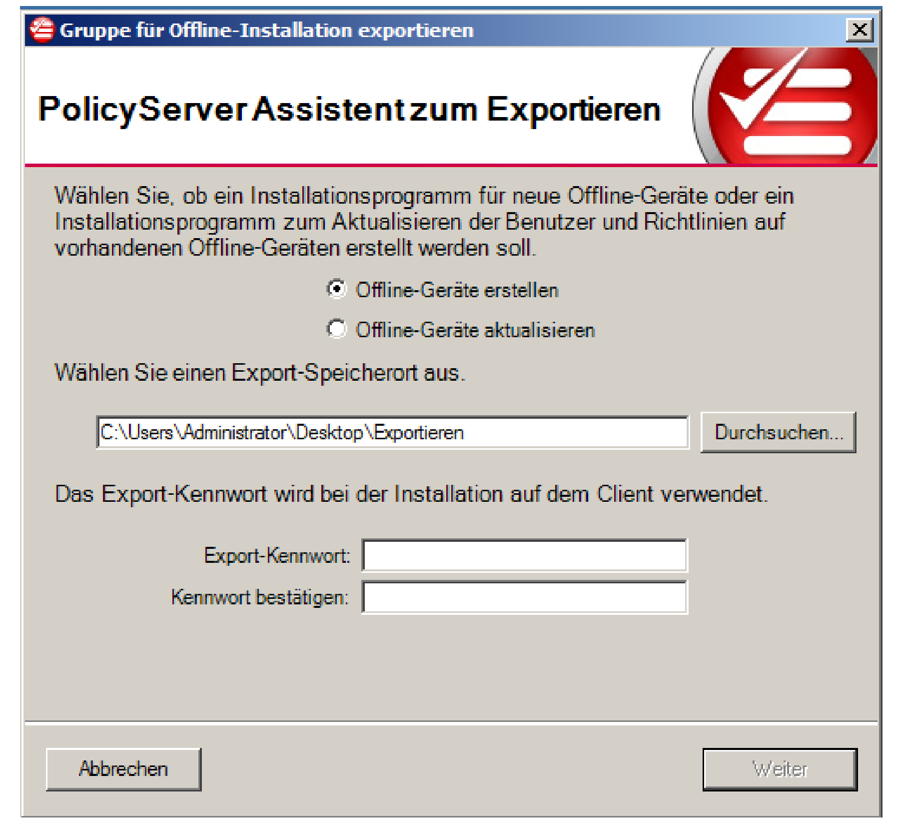


Abbildung 4-3. PolicyServer Assistent zum Exportieren von Gruppen

2. Wählen Sie **Offline-Geräte erstellen** aus, geben Sie den Exportspeicherort und das Exportkennwort ein und klicken Sie auf **Weiter**.



Hinweis

Das Exportkennwort wird zum Authentifizieren der ausführbaren Datei auf dem Endpunkt-Client verwendet.

---

3. Klicken Sie auf **Hinzufügen...**, um zu den Installationsprogrammen des Endpoint Encryption Clients zu navigieren und diese hochzuladen.

TABELLE 4-2. Dateinamen für die Endpoint Encryption Installation

INSTALLATIONSDATEI	ZWECK
`DataArmorInstaller.exe`	Installiert ältere Versionen der Full Disk Encryption Clientanwendung: DataArmor. DataArmor 3.0.12.861 oder früher kann mit Offline-Gruppen verwendet werden. Einzelheiten zu verwalteten Installationen finden Sie im Installationshandbuch.
`TMFDEInstall.exe`	Installiert die Full Disk Encryption Client-Anwendung. Dies gilt nicht für Offline-Geräte. Einzelheiten zu verwalteten Installationen finden Sie im Installationshandbuch.
`FASetup.msi`	Installiert die FileArmor Client-Anwendung für 32-Bit-Betriebssysteme.
`FASetup(x64).msi`	FileArmor Client-Anwendung für 64-Bit-Betriebssysteme.

Fügen Sie so viele Installationsprogramme wie erforderlich hinzu. Eine Gruppe benötigt beispielsweise Full Disk Encryption und FileArmor.

4. Klicken Sie auf **Weiter**.
5. Geben Sie je nach Lizenztyp die Anzahl der zu installierenden Geräte an. Die Anzahl der verfügbaren Lizenzen nimmt mit jedem Gerät ab.
6. Geben Sie optional einen **Präfix des Gerätenamens** an. PolicyServer verwendet die Gerätepräfixnummer, um eine eindeutige Geräte-ID und einen Verschlüsselungsschlüssel für jedes Gerät in dieser Gruppe zu erstellen.
7. Klicken Sie auf **Weiter**.

   Die Offline-Gruppe wird erstellt.
8. Klicken Sie auf **Fertig**, um eine Exportdatei am angegebenen Speicherort zu erstellen.

   Eine erstellte ausführbare Datei namens `Export` wird auf dem Desktop erstellt. Verwenden Sie diese, um Gruppenänderungen an Offline-Clients zu verteilen.

Offline-Gruppe aktualisieren

Führen Sie diese Schritte aus, um eine Aktualisierung für eine Offline-Gruppe zu erstellen.



Warnung!

Führen Sie für Full Disk Encryption Clients, die keine Verbindung zu PolicyServer herstellen, eine nicht verwaltete Installation aus. Richtlinien werden mit der Wiederherstellungskonsole verwaltet.

Prozedur

1. Klicken Sie im linken Fenster mit der rechten Maustaste auf die Gruppe und wählen Sie **Exportieren** aus.

   Der PolicyServer Assistent zum Exportieren von Gruppen wird angezeigt.

2. Wählen Sie **Offline-Geräte erstellen** aus.

3. Geben Sie das Kennwort zum Exportieren ein.

   Hinweis

   Das Exportkennwort wird zum Authentifizieren der ausführbaren Datei auf dem Endpunkt-Client verwendet.

4. Klicken Sie auf **Durchsuchen**, um einen Speicherort anzugeben.

5. Klicken Sie auf **Weiter**.

   Die Offline-Gruppe wird erstellt.

6. Klicken Sie auf **Fertig**.

   Die Exportdatei wird am angegebenen Speicherort erstellt.

7. Installieren Sie die Software auf dem Gerät mit einer generierten ausführbaren Datei oder einem Skript. Weitere Informationen finden Sie im Endpoint Encryption Installationshandbuch.

Arbeiten mit Benutzern

Um identitätsbasierte Authentifizierung bereitzustellen, bietet Endpoint Encryption eine Reihe von unterschiedlichen Benutzerebenen an: Hinzufügen oder Importieren von Benutzer, Zuweisen von Benutzern zu Gruppen, Verwalten von Benutzern und Entfernen von Benutzern.

Benutzer zu PolicyServer hinzufügen

Verwenden Sie die folgenden Methoden, um Benutzer zu Endpoint Encryption hinzuzufügen:

- Fügen Sie die Benutzer manuell nacheinander hinzu.
- Verwenden Sie die Massenimportfunktion für mehrere Benutzer mit einer CSV-Datei.
- Verwenden Sie einen externen Verzeichnis-Browser mit Active Directory.

Neuen Unternehmensbenutzer hinzufügen



Hinweis

- Beim Hinzufügen eines Benutzers zum Unternehmen wird der Benutzer keiner Gruppe zugewiesen.
- Beim Hinzufügen eines Benutzers zu einer Gruppe wird der Benutzer zur Gruppe und zum Unternehmen hinzugefügt.

Prozedur

1. Erweitern Sie das Unternehmen und öffnen Sie **Benutzer**.
2. Klicken Sie mit der rechten Maustaste auf den leeren Bereich im rechten Fenster und wählen Sie **Benutzer hinzufügen** aus.

   Das Fenster **Neuen Benutzer hinzufügen** wird angezeigt.

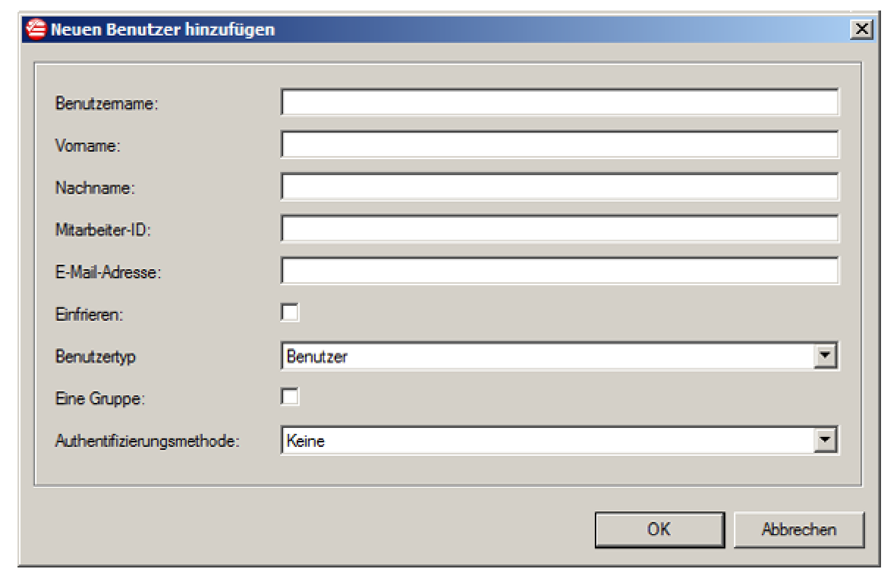


ABBILDUNG 4-4. Fenster "Neuen Benutzer hinzufügen"

3. Geben Sie die Benutzerinformationen ein. Benutzername, Vorname und Nachname sind erforderlich.

4. Wählen Sie nur **Einfrieren** aus, wenn das Konto vorübergehend deaktiviert werden soll. Wenn das Konto eingefroren ist, kann sich der Benutzer nicht an Geräte anmelden.

5. Verwenden Sie das Feld **Benutzertyp**, um die Berechtigungen des neuen Kontos festzulegen. Administratoren und Authentifizierer für das Unternehmen können nicht zu Gruppen hinzugefügt werden.

6. Wählen Sie **Eine Gruppe** aus, um die Mitgliedschaft des Benutzers in mehreren Gruppen zu deaktivieren.

7. Wählen Sie die **Authentifizierungsmethode**.



Hinweis

Die Standardauthentifizierungsmethode für Benutzer lautet **Keine**.

8. Klicken Sie auf **OK**.

Der neue Benutzer wird PolicyServer Enterprise hinzugefügt. Der Benutzer kann erst ein Gerät anmelden, wenn er/sie einer Gruppe hinzugefügt wird.

Benutzer aus einer CSV-Datei importieren

Verwenden Sie eine kommagetrennte Datei (CSV), um mehrere Benutzer gleichzeitig zu importieren.

Verwenden Sie das folgende Format:

`Benutzername (erforderlich), Vorname, Nachname, Mitarbeiter-ID, E-Mail-Adresse`.

Verwenden Sie ein Komma für Felder ohne Daten.



Hinweis

Bei Verwendung der Funktion für den Massenimport von Benutzern werden alle Benutzer in der Datei zur selben Gruppe hinzugefügt. Erstellen Sie eine Datei für jede zu importierende Benutzergruppe.

Prozedur

1. Erweitern Sie die Gruppe im linken Fenster und klicken Sie anschließend auf **Benutzer**.
2. Klicken Sie mit der rechten Maustaste auf den leeren Bereich im rechten Fenster und wählen Sie **Massenimport zum Hinzufügen von Benutzern** aus.

   Das Fenster zum Öffnen der Datei wird angezeigt.
3. Navigieren Sie zur CSV-Datei und klicken Sie auf **Öffnen**.
4. Klicken Sie als Bestätigung auf **OK**.

   Die Benutzer in Ihrer Datei werden zur Gruppe und zum Unternehmen hinzugefügt.

Active Directory-Benutzer importieren

Fügen Sie Active Directory-Benutzer zu vorhandenen PolicyServer Gruppen mit dem externen Verzeichnis-Browser hinzu. PolicyServer beinhaltet ein Benutzerverzeichnis getrennt von der Active Directory-Datenbank. Damit kann PolicyServer absolute Sicherheit für den Zugriff auf alle Geräte, Benutzerrechte und Authentifizierungsmethoden gewährleisten.

Informationen zur Konfiguration der Active Directory-Integration finden Sie im Endpoint Encryption Installationshandbuch.

Prozedur

1. Öffnen Sie im linken Fenster **Unternehmen - Benutzer**, klicken Sie mit der rechten Maustaste auf einen leeren Bereich im linken Fenster und wählen Sie **Externer Verzeichnis-Browser** aus.

   Das Fenster **Active Directory-Benutzerimport** wird angezeigt.

2. Klicken Sie auf **Bearbeiten** > **Mit Domäne verbinden**.

3. Geben Sie den Hostnamen für den Active Directory-LDAP-Server an.

4. Geben Sie einen Benutzernamen und ein Kennwort mit Zugriff auf die Active Directory-Domäne an.

5. Klicken Sie auf **OK**.

   Die Benutzerkonten werden im rechten Fenster geladen.

6. Klicken Sie auf **Datei** und wählen Sie **Zum Unternehmen hinzufügen** oder **Zur Gruppe hinzufügen** aus, je nachdem, wo die Benutzer hinzugefügt werden sollen.

7. Klicken Sie auf **OK**, um die Benutzer zum angegebenen Speicherort hinzuzufügen.

   Ein Bestätigungsfenster wird angezeigt.

8. Klicken Sie zur Bestätigung auf **OK**.

   Eine Importstatusmeldung wird angezeigt.

9. Klicken Sie auf **OK**.

Benutzer suchen

Die Suche nach Benutzern auf Gruppenebene ist zwar schneller, bei dieser Methode muss jedoch das ganze Unternehmen durchsucht werden.

Prozedur

1. Klicken Sie im linken Fenster auf **Unternehmen - Benutzer** oder erweitern Sie die Gruppe und klicken Sie auf **Benutzer**.

2. Klicken Sie in der oberen Ecke des rechten Fensters auf **Suchen**.

Das Fenster **Benutzersuchfilter** wird angezeigt.

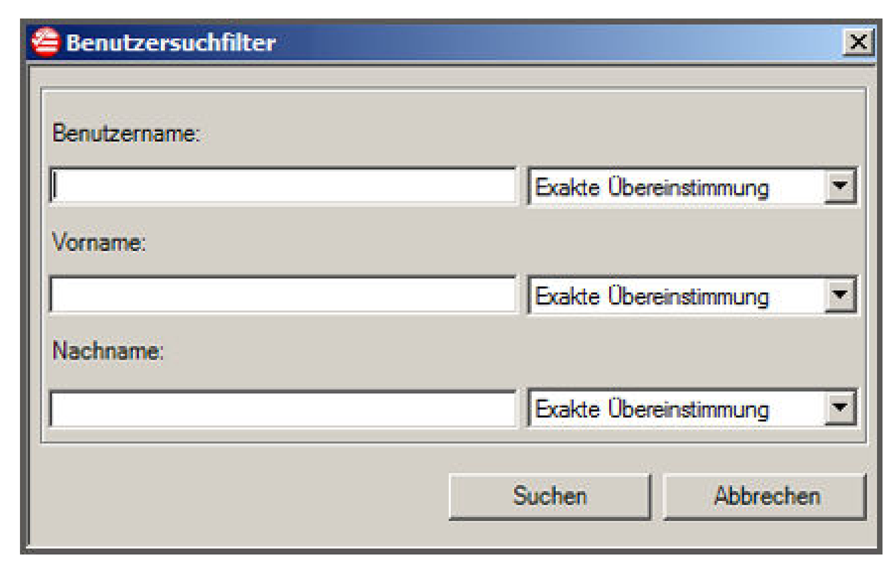


ABBILDUNG 4-5. Fenster "Benutzersuchfilter"

3. Geben Sie die Suchdetails ein und klicken Sie dann auf **Suchen**.

Alle mit diesem Suchkriterium übereinstimmenden Konten werden angezeigt.



Hinweis

Verwenden Sie bei vielen Benutzern die Option **Seitenzähler**, um von einer Seite zur anderen zu wechseln, und klicken Sie auf **Löschen**, um alle Ergebnisse zu entfernen.

Benutzer ändern

Jeder Gruppenadministrator kann die Profilinformationen eines Benutzers ändern.



Hinweis

- Änderungen auf Unternehmensebene werden global auf den Benutzer angewendet, wohingegen sich Änderungen auf Gruppenebene nur auf eine bestimmte Gruppe beziehen.

Prozedur

1. Öffnen Sie **Unternehmen - Benutzer**.
2. Klicken Sie im rechten Fenster mit der rechten Maustaste auf den Benutzer und wählen Sie **Benutzer ändern** aus.

   Das Fenster **Benutzer ändern** wird angezeigt.
3. Nehmen Sie die erforderlichen Änderungen vor. Wenn sich die Authentifizierungsmethoden-Änderungen in **Festes Kennwort** ändern, geben Sie das Standardbenutzerkennwort an.
4. Klicken Sie auf **OK**.
5. Wenn die Bestätigungsmeldung angezeigt wird, klicken Sie auf **OK**.

Gruppenmitgliedschaft eines Benutzers anzeigen

Wenn ein Benutzer mehreren Gruppen angehört, können diese von einem Administrator angezeigt werden.

Prozedur

1. Öffnen Sie **Unternehmen - Benutzer**.
2. Klicken Sie mit der rechten Maustaste auf den Benutzer und wählen Sie **Gruppen auflisten** aus.

   Die Liste **Gruppenmitgliedschaft** wird angezeigt.

Neuen Benutzer zu einer Gruppe hinzufügen



Hinweis

- Beim Hinzufügen eines Benutzers zum Unternehmen wird der Benutzer keiner Gruppe zugewiesen.
- Beim Hinzufügen eines Benutzers zu einer Gruppe wird der Benutzer zur Gruppe und zum Unternehmen hinzugefügt.

Prozedur

1. Erweitern Sie die Gruppe und öffnen Sie **Benutzer**.
2. Klicken Sie mit der rechten Maustaste auf den leeren Bereich im rechten Fenster und wählen Sie **Neuen Benutzer hinzufügen** aus.

   Das Fenster **Neuen Benutzer hinzufügen** wird angezeigt.

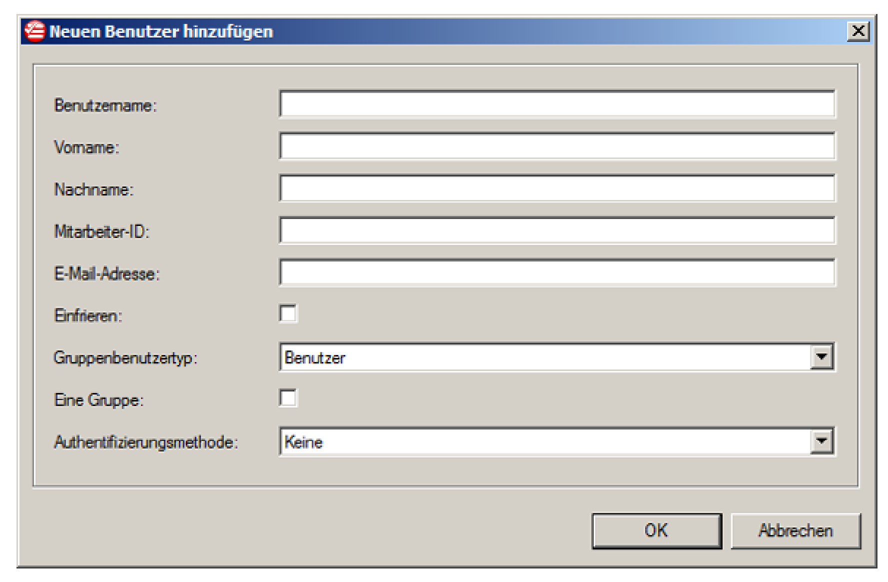


ABBILDUNG 4-6. Fenster "Neuen Benutzer hinzufügen"

3. Geben Sie die Benutzerinformationen ein. Benutzername, Vorname und Nachname sind erforderlich.

4. Wählen Sie nur **Einfrieren** aus, wenn das Konto vorübergehend deaktiviert werden soll. Wenn das Konto eingefroren ist, kann sich der Benutzer nicht an Geräte anmelden.

5. Verwenden Sie das Feld **Gruppenbenutzertyp**, um die Berechtigungen des neuen Kontos festzulegen. Administratoren und Authentifizierer für das Unternehmen können nicht zu Gruppen hinzugefügt werden.

6. Wählen Sie **Eine Gruppe** aus, um die Mitgliedschaft des Benutzers in mehreren Gruppen zu deaktivieren.

7. Wählen Sie die **Authentifizierungsmethode**.



Hinweis

Die Standardauthentifizierungsmethode für Benutzer lautet **Keine**.

8. Klicken Sie auf **OK**.

Der neue Benutzer wird der ausgewählten Gruppe **und** zum Unternehmen hinzugefügt. Der Benutzer kann sich jetzt ein Gerät anmelden.

Vorhandenen Benutzer zu einer Gruppe hinzufügen

Ein Benutzer kann zu mehreren Gruppen hinzugefügt werden.

Prozedur

1. Erweitern Sie die Gruppe im linken Fenster und klicken Sie anschließend auf **Benutzer**.
2. Klicken Sie mit der rechten Maustaste auf den leeren Bereich im rechten Fenster und wählen Sie **Vorhandenen Benutzer hinzufügen** aus.

   Das Fenster **Benutzer zu Gruppe hinzufügen** wird angezeigt.

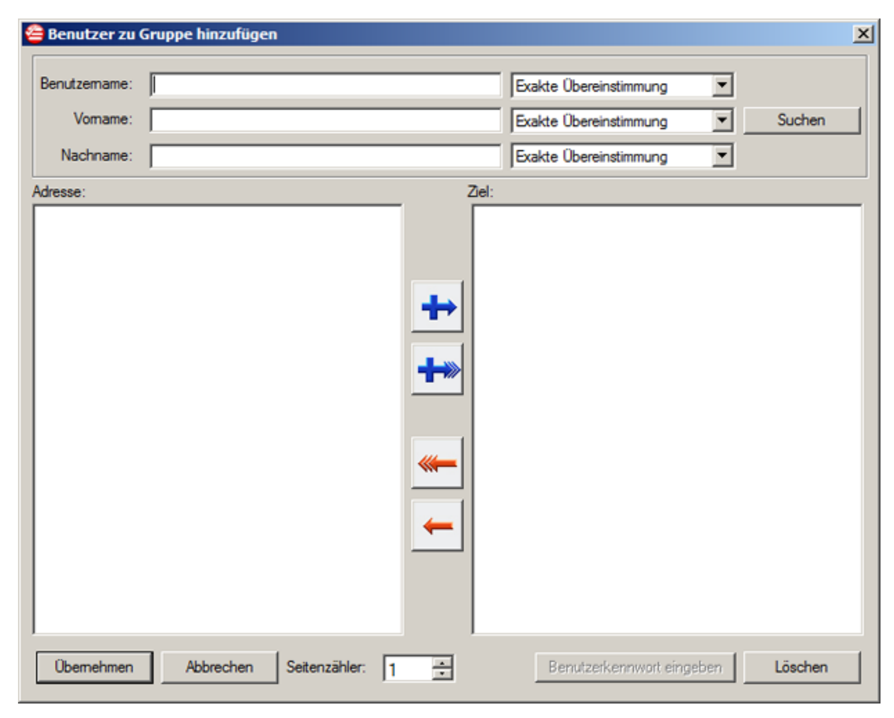


ABBILDUNG 4-7. Fenster "Vorhandenen Benutzer zu Gruppe hinzufügen"

3. Geben Sie die Benutzerdetails ein und klicken Sie dann auf **Suchen**.

   Wird eine Übereinstimmung gefunden, werden im Feld **Quelle** Konten angezeigt.

4. Wählen Sie Benutzerkonten aus der Liste aus und klicken Sie auf den **blauen Pfeil**, um sie hinzuzufügen. Weitere Steuerelemente finden Sie unter *Kapitel 2, Tabelle 2-3: Symbole zum Hinzufügen/Entfernen von Benutzern auf Seite 2-13*.

TABELLE 4-3. Symbole zum Hinzufügen/Entfernen von Benutzern

ZENTRALE SYMBOLE	BESCHREIBUNG
	Fügt einen einzelnen ausgewählten Benutzer zum Feld **Ziel** hinzu.

Zentrale Symbole	Beschreibung
	Fügt alle gefundenen Benutzer basierend auf Suchkriterien zum Feld **Ziel** hinzu.
	Löscht einen einzelnen ausgewählten Benutzer im Feld **Ziel**.
	Löscht alle Benutzer im Feld **Ziel**.

5. So ändern Sie ein Benutzerkennwort:

a. Markieren Sie den Benutzer im Feld **Ziel**.

b. Klicken Sie im unteren Fensterbereich auf **Benutzerkennwort eingeben**.

c. Geben Sie im anschließend angezeigten Fenster die Authentifizierungsmethode für den Benutzer an.

d. Klicken Sie auf **Übernehmen**.

6. Klicken Sie auf **Übernehmen**.

Der Benutzer wird zur Gruppe hinzugefügt. Wenn dies die einzige Gruppe ist, zu der der Benutzer gehört, kann sich der Benutzer nun beim Endpunkt-Client anmelden.

Standardgruppe eines Benutzers ändern

Die erste Gruppe in der Liste ist die Standardgruppe für den Benutzer.



Hinweis

Der Benutzer muss dazu berechtigt sein, in die Standardgruppe zu installieren. Weitere Informationen finden Sie unter *Benutzer das Installieren in eine Gruppe erlauben auf Seite 4-21*.

.

Prozedur

1. Öffnen Sie **Unternehmen - Benutzer**.
2. Klicken Sie mit der rechten Maustaste auf den Benutzer und wählen Sie dann **Gruppen auflisten** aus.

   Die Liste **Gruppenmitgliedschaft** wird angezeigt.
3. Klicken Sie mit der rechten Maustaste auf den Benutzer und wählen Sie dann **An den Anfang verschieben** aus.

   Die Standardgruppe des Benutzers wurde geändert.

Benutzer das Installieren in eine Gruppe erlauben

Mit dieser Option können Benutzer ohne die Zustimmung eines Administrators Endpoint Encryption Geräte in eine Gruppe installieren, in der sie Mitglied sind.



Hinweis

Die Standardeinstellung lautet **Benutzer das Installieren in diese Gruppe nicht erlauben**.

Prozedur

1. Öffnen Sie **Unternehmen - Benutzer**.
2. Klicken Sie mit der rechten Maustaste auf den Benutzer und wählen Sie dann **Gruppen auflisten** aus.

   Die Liste **Gruppenmitgliedschaft** wird angezeigt.
3. Klicken Sie mit der rechten Maustaste auf den Benutzer und wählen Sie **Benutzer das Installieren in diese Gruppe erlauben** aus.

   Der Benutzer kann jetzt Geräte in diese Gruppe installieren.

Einzelne Benutzer aus einer Gruppe entfernen



Warnung!

Bevor Sie einen Gruppenadministrator oder Authentifiziererkonto entfernen, weisen Sie diese Rolle einem anderen Benutzer zu. Andernfalls können nur Administratoren oder Authentifikatoren auf der Unternehmensebene Änderungen auf Gruppenebene vornehmen.

Prozedur

1. Erweitern Sie die Gruppe und klicken Sie auf **Benutzer**.
2. Klicken Sie im rechten Fenster mit der rechten Maustaste auf den Benutzer und wählen Sie **Benutzer entfernen** aus.

   Eine Warnmeldung wird angezeigt.
3. Um den Benutzer ebenfalls vom Unternehmen zu entfernen, aktivieren Sie das Kontrollkästchen **Von Unternehmen entfernen**.

   Hinweis

   Beim Entfernen eines Benutzers vom Unternehmen wird der Benutzer ebenfalls aus allen Gruppen und Untergruppen entfernt.
4. Klicken Sie auf **Ja**.

   Der Benutzer wird entfernt.

Alle Benutzer aus einer Gruppe entfernen



Warnung!

Bevor Sie einen Gruppenadministrator oder Authentifiziererkonto entfernen, weisen Sie diese Rolle einem anderen Benutzer zu. Andernfalls können nur Administratoren oder Authentifikatoren auf der Unternehmensebene Änderungen auf Gruppenebene vornehmen.

Prozedur

1. Erweitern Sie die Gruppe, und klicken Sie anschließend auf **Benutzer**.
2. Klicken Sie im rechten Fenster mit der rechten Maustaste auf den Benutzer und wählen Sie **Alle Benutzer entfernen** aus.

   Eine Warnmeldung wird angezeigt.
3. Um alle Benutzer ebenfalls vom Unternehmen zu entfernen, aktivieren Sie das Kontrollkästchen **Von Unternehmen entfernen**.

   
   Hinweis

   Beim Entfernen eines Benutzers vom Unternehmen wird der Benutzer ebenfalls aus allen Gruppen und Untergruppen entfernt.
4. Klicken Sie auf **Ja**.

Gelöschtes Benutzer wiederherstellen

Alle gelöschten Benutzer werden im Papierkorb auf der Unternehmensebene gespeichert. Gruppen haben keinen Papierkorb. Bei der Wiederherstellung eines Benutzers wird der Benutzer nicht wieder zu den zuvor zugewiesenen Gruppen hinzugefügt.

Prozedur

1. Erweitern Sie den Papierkorb.
2. Öffnen Sie **Gelöschte Benutzer**.

   Im rechten Fenster werden alle gelöschten Benutzer geladen.
3. Klicken Sie mit der rechten Maustaste auf den Benutzer und wählen Sie **Benutzer wiederherstellen** aus.

Der Benutzer wird zum Unternehmen hinzugefügt, gehört jedoch keiner Gruppe an.

Arbeiten mit Kennwörtern

Wenn ein Benutzer sein Kennwort vergisst oder ein Gerät verlegt, kann er sein Kennwort mit den in Unternehmens- oder Gruppenrichtlinien definierten Methoden zurücksetzen. Die folgenden Methoden zum Zurücksetzen von Kennwörtern stehen zur Verfügung:

- Microsoft Windows Active Directory
- PolicyServer MMC
- Remote-Hilfe
- Selbsthilfe

Bei allen genannten Optionen ist es erforderlich, die Richtlinie auf Unternehmensebene und je nach Bedarf auf Gruppenebene festzulegen. Verwenden Sie die Richtlinie "Support-Informationen", um Benutzern Informationen zum Zurücksetzen von Kennwörtern zur Verfügung zu stellen.

Unternehmensadministrator-/Authentifiziererkennwort zurücksetzen

Nur Unternehmensadministratoren können Kennwörter für einen Unternehmensadministrator zurücksetzen. Ein Authentifizierer mit denselben Gruppenberechtigungen oder mehr kann ein Administrator- oder Authentifiziererkennwort innerhalb dieser Gruppe zurücksetzen.



Tipp

Trend Micro empfiehlt das dauerhafte Vorhandensein von mindestens drei Unternehmensadministratorkonten, um dem Verlust von Kennwörtern vorzubeugen. Wenn ein Kennwort für ein Unternehmensadministratorkonto verloren geht, kann es mit der Selbsthilfe möglicherweise zurückgesetzt werden.

Prozedur

1. Melden Sie sich bei der PolicyServer MMC mit einem Unternehmensadministratorkonto an.
2. Öffnen Sie **Unternehmen - Benutzer**.
3. Klicken Sie mit der rechten Maustaste auf das Unternehmensadministrator- oder Authentifiziererkonto mit dem verlorenen Kennwort und wählen Sie **Kennwort ändern** aus.

   Das Fenster **Kennwort ändern** wird angezeigt.
4. Wählen Sie eine Authentifikationsmethode aus.
5. Geben Sie das Kennwort ein (falls erforderlich).
6. Klicken Sie auf **Übernehmen**.

   Das Kontokennwort wird zurückgesetzt.



Hinweis

Die Option **Benutzer muss Kennwort bei nächster Anmeldung ändern** ist nur nach der Aktualisierung der Richtlinien auf dem Endpunkt-Client verfügbar.

Gruppenadministrator-/Authentifiziererkennwort zurücksetzen

Alle Kennwortänderungen gelten nur für die jeweilige Gruppe. Wenn ein Administrator nur ein Kennwort haben möchte, sollte er nur einer Top-Gruppe angehören.

Prozedur

1. Melden Sie sich bei der PolicyServer MMC mit einem Gruppenadministratorkonto an.
2. Erweitern Sie die Gruppe und öffnen Sie **Benutzer**.

3. Klicken Sie mit der rechten Maustaste auf das Gruppenadministrator- oder Authentifiziererkonto mit dem verlorenen Kennwort und wählen Sie **Kennwort ändern** aus.

   Das Fenster **Kennwort ändern** wird angezeigt.

4. Wählen Sie eine Authentifikationsmethode aus.

5. Geben Sie das Kennwort ein und bestätigen Sie es (falls erforderlich).

6. Klicken Sie auf **Übernehmen**.

   Das Kontokennwort wird zurückgesetzt.



Hinweis

Die Option **Benutzer muss Kennwort bei nächster Anmeldung ändern** ist nur nach Client-Aktualisierungen verfügbar.

Benutzerkennwort zurücksetzen

Aktivieren Sie beim Zurücksetzen eines Benutzerkennworts das Kontrollkästchen **Benutzer muss Kennwort bei nächster Anmeldung ändern**, damit ein Benutzer sein Kennwort ändern muss, wenn er sich das nächste Mal anmeldet. Wenn sich der Benutzer anmeldet und er das Kennwort ändert, muss er ebenfalls das Kennwort für alle Geräte ändern.



Hinweis

Trend Micro empfiehlt die Verwendung der Domänenauthentifizierung.

Auf ein festes Kennwort zurücksetzen

Prozedur

1. Öffnen Sie **Unternehmen - Benutzer** oder erweitern Sie eine Gruppe und öffnen Sie **Benutzer**.

2. Wählen Sie die Benutzer aus dem rechten Fenster aus.

Halten Sie die Umschalttaste gedrückt, um mehrere Benutzer auszuwählen. Die Mehrfachauswahl ist nur auf der Gruppenebene möglich.

3. Klicken Sie mit der rechten Maustaste und wählen Sie **Kennwort ändern** aus.

   Das Fenster **Kennwort ändern** wird angezeigt.

4. Wählen Sie als **Authentifizierungsmethode** den Eintrag **Festes Kennwort** aus.

5. Geben Sie das Kennwort ein und bestätigen Sie es.

6. Klicken Sie auf **Übernehmen**.

   Bei der nächsten Anmeldung muss der Benutzer sein Kennwort ändern.

Benutzerkennwort mit Active Directory zurücksetzen

Trend Micro empfiehlt die Verwendung von Active Directory zum Zurücksetzen des Benutzerkennworts, besonders dann, wenn der Benutzer Zugriff auf das Helpdesk des Unternehmens hat, über eine Netzwerkverbindung verfügt oder wenn Windows Single-Sign-On (SSO) aktiviert ist.

Weitere Informationen zum Zurücksetzen eines Domänenbenutzerkennworts mit Active Directory finden Sie im Handbuch zum jeweiligen Windows Betriebssystem.

Selbsthilfe-Kennwortunterstützung verwenden

Mit dieser Aufgabe wird die Konfiguration von Richtlinien für Selbsthilfe beschrieben. Benutzer, die ihre Kennwörter vergessen haben, können die Selbsthilfe verwenden, ohne die Unterstützung durch das Helpdesk für die Authentifizierung anzufordern. Verwenden Sie die Richtlinien "Anzahl der Fragen" und "Persönliche Herausforderung", um die persönlichen Herausforderungsfragen und die Fragen, die der Benutzer beantworten muss, festzulegen. Selbsthilfefragen werden bei der ersten Benutzerauthentifizierung und wenn Benutzer ihre Kennwörter ändern beantwortet.

Details zur Verwendung der Selbsthilfe finden Sie unter *Selbsthilfe auf Seite 1-19*.



Hinweis

Für die Selbsthilfe ist eine Netzwerkverbindung zu PolicyServer erforderlich.

Prozedur

1. Erweitern Sie **Unternehmen - Richtlinien** oder erweitern Sie die Gruppe und dann **Richtlinien**.

2. Navigieren Sie zu **Allgemein** > **Authentifizierung** > **Lokale Anmeldung** > **Selbsthilfe**.

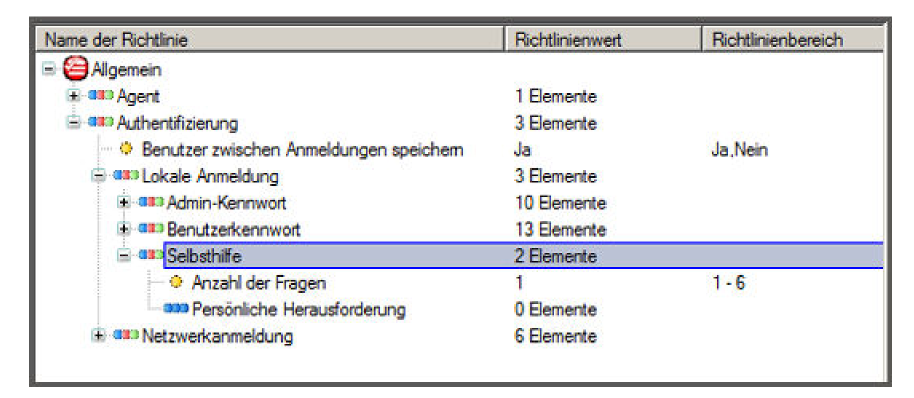


ABBILDUNG 4-8. Selbsthilfe-Richtlinie

3. Öffnen Sie **Anzahl der Fragen**, um die erforderliche Anzahl an Fragen festzulegen, die die Benutzer beantworten müssen.



Warnung!

Legen Sie für **Anzahl der Fragen** keinen Wert größer als 6 fest. Andernfalls können sich die Benutzer nicht anmelden.

4. Klicken Sie mit der rechten Maustaste auf **Persönliche Herausforderung** und wählen Sie **Hinzufügen** aus, um eine Frage festzulegen, die der Benutzer beantworten muss. Wiederholen Sie diesen Vorgang, bis alle persönlichen Herausforderungsfragen festgelegt sind.

   Wenn sich die Benutzer das nächste Mal anmelden, werden Sie aufgefordert, ihre persönliche Herausforderungsfrage zu beantworten.

Remote-Hilfe für Kennwort-Support

Vergessene Kennwörter mit Remote-Hilfe zurücksetzen. Ein Benutzer, dessen Konto gesperrt ist oder der sein Kennwort vergessen hat, muss sein Kennwort zurücksetzen, bevor er sich mit einem neuen Kennwort anmeldet. Remote-Hilfe setzt voraus, dass der Benutzer beim Helpdesk eine Herausforderungsantwort anfordert. Für die Remote-Hilfe ist keine Netzwerkverbindung zu PolicyServer erforderlich.

Prozedur

1. Melden Sie sich bei der PolicyServer MMC mit einem Enterprise Administratorkonto oder einem Gruppenadministrator-/Authentifiziererkonto innerhalb derselben Richtliniengruppe wie der Benutzer an.

2. Fordern Sie den Benutzer auf, auf seinem Endpunkt-Client auf **Hilfe** > **Remote-Hilfe** zu klicken.

3. Fragen Sie den Benutzer nach der angezeigten **Geräte-ID**.

ABBILDUNG 4-9. Unterstützung durch Remote-Hilfe

4. Öffnen Sie in der PolicyServer MMC **Unternehmen - Geräte** oder erweitern Sie die Benutzergruppe und klicken Sie auf das Symbol **Geräte** in der Benutzergruppe.

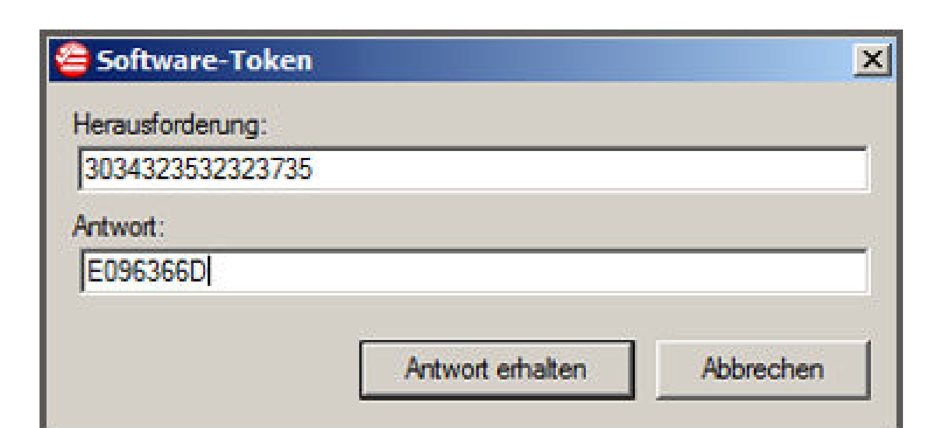
5. Klicken Sie im rechten Fenster mit der rechten Maustaste auf das Benutzergerät und wählen Sie **Soft-Token** aus.

   Das Fenster **Soft-Token** wird angezeigt.

6. Fordern Sie den Benutzer auf, das aus 16 Ziffern bestehende Feld **Herausforderung** zu lesen, und geben Sie es im Feld **Herausforderung** im Fenster **Software-Token** ein.

7. Klicken Sie auf **Antwort erhalten**.

Das Feld **Antwort** wird mit einer aus 8 Zeichen bestehenden Zeichenfolge geladen.



8. Teilen Sie dem Benutzer die aus 8 Zeichen bestehende Zeichenfolge über das Feld **Antwort** mit.

9. Der Benutzer gibt die Zeichenfolge im Feld **Antwort** am Endpunkt ein und klickt auf **Anmelden**.

10. Der Benutzer wird zur Eingabe eines neuen Kennworts aufgefordert.

Setup für Support-Informationen

Die Richtlinie für Support-Informationen gibt Informationen zum Support-Helpdesk eines Unternehmens an. Die Richtlinie für Support-Informationen kann für jede Gruppe individuell konfiguriert werden.

Prozedur

1. Melden Sie sich bei der PolicyServer MMC mit einem Enterprise Administratorkonto oder einem Gruppenadministrator-/Authentifiziererkonto innerhalb derselben Richtliniengruppe wie der Benutzer an.

2. Erweitern Sie die Benutzergruppe und navigieren Sie zu **Richtlinien** > **Full Disk Encryption** > **Allgemein** > **Anmelden**.

3. Klicken Sie mit der rechten Maustaste auf die Richtlinie **Support-Informationen** und wählen Sie **Hinzufügen** aus.

4. Geben Sie Support-Informationen an (Telefonnummer, Standort).

5. Klicken Sie auf **OK**.

Arbeiten mit Geräten

Geräte sind Computer, Laptops, Smartphones und alle anderen Endpunkte, auf denen Full Disk Encryption, FileArmor oder KeyArmor installiert ist. Geräte werden automatisch zum Unternehmen hinzugefügt, wenn eine beliebige Endpoint Encryption Anwendung installiert wird.



Hinweis

Jedes Gerät kann nur Teil einer Gruppe sein.

Gerät zu einer Gruppe hinzufügen

Prozedur

1. Erweitern Sie im linken Fenster die gewünschte Richtliniengruppe und klicken Sie auf **Geräte**.

2. Klicken Sie im rechten Fenster mit der rechten Maustaste auf das Gerät und wählen Sie **Gerät hinzufügen** aus.

Das Fenster **Geräte zu Gruppe hinzufügen** wird angezeigt.

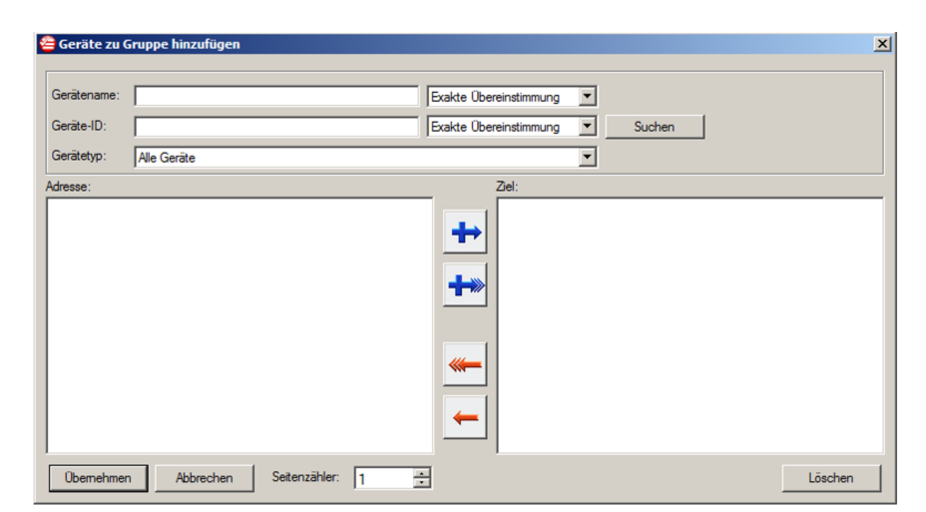


ABBILDUNG 4-10. Fenster Geräte zu Gruppe hinzufügen

3. Geben Sie die Gerätedetails ein und klicken Sie dann auf **Suchen**.

Wird eine Übereinstimmung gefunden, werden im Feld **Quelle** Konten angezeigt.

4. Wählen Sie das Gerät aus der Liste aus und klicken Sie auf den **blauen Pfeil**, um es hinzuzufügen. Weitere Steuerelemente finden Sie in der Tabelle.

TABELLE 4-4. Symbole zum Hinzufügen/Entfernen von Geräten

ZENTRALE SYMBOLE	BESCHREIBUNG
	Fügt ein einzelnes ausgewähltes Gerät zum Feld **Ziel** hinzu.
	Fügt alle gefundenen Geräte basierend auf Suchkriterien zum Feld **Ziel** hinzu.

ZENTRALE SYMBOLE	BESCHREIBUNG
	Löscht ein einzelnes ausgewähltes Gerät im Feld **Ziel**.
	Löscht alle Geräte im Feld **Ziel**.

5. Klicken Sie auf **Anwenden**, um das Gerät zur ausgewählten Gruppe hinzuzufügen.

   Das Gerät wird zur Gruppe hinzugefügt.

Gerät aus einer Gruppe entfernen

Beim Löschen eines Geräts aus einer Gruppe wird das Gerät nur aus der ausgewählten Gruppe entfernt.



Warnung!

Um ein Gerät aus allen Gruppen zu entfernen, entfernen Sie es aus dem Unternehmen. Stellen Sie vor dem Löschen eines Geräts aus dem Unternehmen sicher, dass das Gerät entschlüsselt wurde und alle Trend Micro Produkte deinstalliert wurden. Falls Sie dies nicht tun, könnte dies zu irreversiblen Datenverlusten führen.

Prozedur

1. Erweitern Sie die Gruppe und öffnen Sie **Geräte**.
2. Klicken Sie im rechten Fenster mit der rechten Maustaste auf das Gerät und wählen Sie **Gerät entfernen** aus.

   Eine Warnmeldung wird angezeigt.

3. Klicken Sie auf **Ja**.

Das Gerät wird entfernt.

Gerät aus dem Unternehmen entfernen

Beim Löschen eines Geräts aus dem Unternehmen wird das Gerät aus allen Gruppen und aus dem Unternehmen entfernt. Das Gerät funktioniert, solange die Richtlinen für Konnektivität und Kennwort auf dem Gerät aktuell sind. Dateien können nicht wiederhergestellt werden, wenn das Gerät in diesem Status fehlschlägt. Um dieses Risiko zu vermeiden, entschlüsseln Sie das Gerät sofort, deinstallieren Sie Full Disk Encryption und installieren Sie Full Disk Encryption anschließend als einen nicht verwalteten Client neu.



Warnung!

Überprüfen Sie, ob die Verschlüsselung des Geräts aufgehoben und alle Trend Micro Anwendungen deinstalliert wurden, beovr ein Gerät aus dem Unternehmen gelöscht wird. Falls Sie dies nicht tun, könnte dies zu irreversiblen Datenverlusten führen.

Informationen zum Entfernen eines Geräts aus einer bestimmten Gruppe aber nicht aus dem Unternehmen finden Sie unter *Gerät aus einer Gruppe entfernen auf Seite 4-34*.



Hinweis

Navigieren Sie zum Papierkorb, um ein entferntes Gerät erneut zum Unternehmen hinzuzufügen.

Prozedur

1. Deinstallieren Sie die Endpunkt-Clientanwendung vom Gerät. Informationen zur Deinstallation des Endpunkt-Clients finden Sie im Endpoint Encryption Installationshandbuch.
2. Öffnen Sie **Unternehmen - Geräte**.
3. Klicken Sie im rechten Fenster mit der rechten Maustaste auf das Gerät und wählen Sie **Gerät entfernen** aus. Klicken Sie auf das ausgewählte Gerät.

   Eine Warnmeldung wird angezeigt.

4. Klicken Sie auf **Ja**.

   Das Gerät wird entfernt.

Verzeichnisinhalte anzeigen

Verwenden Sie die Verzeichnislistenoption, um ein Snapshot aller auf das ausgewählte Gerät heruntergeladenen Anwendungen anzuzeigen.

Prozedur

1. Öffnen Sie **Unternehmen - Geräte** oder erweitern Sie eine Gruppe und öffnen Sie **Geräte**.
2. Klicken Sie im rechten Fenster mit der rechten Maustaste auf das Gerät und wählen Sie **Verzeichnisüberwachung** aus.

   Das Fenster **Snapshot des Geräteverzeichnisses** zeigt alle auf das Gerät heruntergeladenen Anwendungen an.

Geräteattribute anzeigen

Verwenden Sie die Option "Geräteattribute" (Speicher, Betriebssystem, Akkustand usw.), um einen aktuellen Snapshot des ausgewählten Geräts anzuzeigen.

Prozedur

1. Öffnen Sie **Unternehmen - Geräte** oder erweitern Sie eine Gruppe und öffnen Sie **Geräte**.
2. Klicken Sie im rechten Fenster mit der rechten Maustaste auf das Gerät und wählen Sie **Verzeichnisüberwachung** aus.

Das Fenster **Geräteattribute** wird angezeigt.

Geräteattribute

Name:	Wert
Disk Model	VMware, VMware Virtual S SCSI Disk Device
Disk Name	\\.\PHYSICALDRIVE0
Disk Partitions	1
Disk Size	64420392960
Domain Name	WORKGROUP
Drive Percent Encrypted	0,69%
Full Disk Encryption user	dauser
Full Disk Encryption Version	3.1.3.252
Hostname	WIN-A053D33LGTI
IP Address	fe80::81aa:29f1:c5e2:a63d%11;fe80::2c76:1d34:53ef:e5e0%13;172.16.2
Last Updated (UTC)	2012-10-17 03:51:04Z
Locale	Deutsch (Deutschland)
Operating System	Microsoft Windows NT 6.1.7601 Service Pack 1
Operating System Name	Microsoft Windows 7 Home Basic
Operating System Service Pack	Service Pack 1
Operating System Version	6.1.7601.65536

ABBILDUNG 4-11. Geräteattributliste

Verzeichnisüberwachung anzeigen

Verwenden Sie die Verzeichnisüberwachung, um nur die Verzeichnisstruktur von KeyArmor-Geräten anzuzeigen.

Prozedur

1. Öffnen Sie **Unternehmen - Geräte** oder erweitern Sie eine Gruppe und öffnen Sie **Geräte**.

2. Klicken Sie im rechten Fenster mit der rechten Maustaste auf das Gerät und wählen Sie **Verzeichnisüberwachung** aus.

   Das Fenster **Snapshot des Geräteverzeichnisses** wird angezeigt.

Gerät auslöschen

Beim Auslöschen eines Geräts werden alle Daten komplett gelöscht. Für DriveArmor, Full Disk Encryption und KeyArmor wird der Befehl zum Auslöschen ausgegeben, wenn das Gerät mit PolicyServer kommuniziert.



Warnung!

Das Auslöschen eines Geräts kann nicht rückgängig gemacht werden. Sichern Sie alle Daten, bevor Sie diese Aktion durchführen.

Prozedur

1. Öffnen Sie **Unternehmen - Geräte** oder erweitern Sie eine Gruppe und öffnen Sie **Geräte**.
2. Klicken Sie im rechten Fenster mit der rechten Maustaste auf das Gerät und wählen Sie **Gerät auslöschen** aus.
3. Klicken Sie auf **Ja**, wenn die Warnmeldung angezeigt wird.
4. Wenn die Bestätigungsmeldung angezeigt wird, klicken Sie auf **OK**.

Gerät sperren

Beim Sperren eines Gerät wird das Gerät neu gestatet und in einen Status gezwungen, der Remote-Hilfe erfordert. Für DriveArmor, Full Disk Encryption und KeyArmor wird der Sperrbefehl ausgegeben, wenn das Gerät mit PolicyServer kommuniziert.

Sperren Sie ein Gerät, um zu verhindern, dass sich ein Benutzer erst dann beim Gerät authentifiziert, wenn eine Remote-Hilfe-Authentifizierung erfolgreich durchgeführt wurde.

Prozedur

1. Öffnen Sie **Unternehmen - Geräte** oder erweitern Sie eine Gruppe und öffnen Sie **Geräte**.

2. Klicken Sie im rechten Fenster mit der rechten Maustaste auf das Gerät und wählen Sie **Gerät sperren** aus.

3. Klicken Sie auf **Ja**, wenn die Warnmeldung angezeigt wird.

4. Wenn die Bestätigungsmeldung angezeigt wird, klicken Sie auf **OK**.

Gerät neu starten

Führen Sie einen Warmstart durch, um ein Gerät neu zu starten. Für DriveArmor, Full Disk Encryption und KeyArmor wird der Warmstartbefehl ausgegeben, wenn das Gerät mit PolicyServer kommuniziert.

Prozedur

1. Öffnen Sie **Unternehmen - Geräte** oder erweitern Sie eine Gruppe und öffnen Sie **Geräte**.

2. Klicken Sie im rechten Fenster mit der rechten Maustaste auf das Gerät und wählen Sie **Warmstart** aus.

3. Klicken Sie auf **Ja**, wenn die Warnmeldung angezeigt wird.

4. Wenn die Bestätigungsmeldung angezeigt wird, klicken Sie auf **OK**.

Gelöschtes Gerät wiederherstellen

Alle gelöschten Geräte werden im Papierkorb auf der Unternehmensebene gespeichert. Gruppen haben keinen Papierkorb. Bei der Wiederherstellung eines Geräts wird das Gerät nicht wieder zu den zuvor zugewiesenen Gruppen hinzugefügt.

Prozedur

1. Erweitern Sie den Papierkorb.

2. Öffnen Sie **Gelöschte Geräte**.

   Im rechten Fenster werden alle gelöschten Benutzer geladen.

3. Klicken Sie mit der rechten Maustaste auf das Gerät und wählen Sie **Gerät wiederherstellen** aus.

   Das Gerät wird zum Unternehmen hinzugefügt, gehört jedoch keiner Gruppe an.



Kapitel 5

Mit Full Disk Encryption arbeiten

Mit Hilfe von obligatorischer starker Authentifizierung und Full Disk Encryption bietet Full Disk Encryption eine umfassende Endpunkt-Datensicherheit. Full Disk Encryption sichert nicht nur die Datendateien, sondern darüber hinaus alle Anwendungen, Registrierungseinstellungen, temporären Dateien, Auslagerungsdateien, Druck-Spooler und gelöschten Dateien. Eine starke Preboot-Authentifizierung beschränkt den Zugriff auf das anfällige Host-Betriebssystem, bis der Benutzer validiert wird.

Dieses Kapitel umfasst folgende Themen:

- *Endpoint Encryption Tools auf Seite 5-2*
- *Full Disk Encryption Preboot Authentifizierung auf Seite 5-2*
- *Full Disk Encryption Konnektivität auf Seite 5-15*
- *Full Disk Encryption – Wiederherstellungskonsole auf Seite 5-16*
- *Full Disk Encryption Wiederherstellungsmethoden auf Seite 5-27*
- *Reparatur-CD auf Seite 5-29*

Endpoint Encryption Tools

TABELLE 5-1. Endpoint Encryption Tools

TOOL	ZWECK
Wiederherstellungskonsole	• Wiederherstellung eines Geräts beim Ausfall des primären Betriebssystems. • Fehlerbehebung bei Netzwerkproblemen • Verwaltung von Benutzern und Protokollen
Command Line Helper	• Mit dem Command Line Helper können verschlüsselte Werte erzeugt werden, die als sichere Anmeldedaten beim Erstellen von Installationsskripts verwendet werden können.
Command Line Installer Helper	• Erstellen von Skripts für automatische Installationen. • Mit dem Command Line Helper können verschlüsselte Werte erzeugt werden, die als sichere Anmeldedaten beim Erstellen von Installationsskripts verwendet werden können.
DAAutoLogin	• Für Windows-Patches verwendet. Mit DAAutoLogin kann Endpoint Encryption Preboot einmalig umgangen werden.
Reparatur-CD	• Verwenden Sie diese startfähige CD, um das Laufwerk zu entschlüsseln, bevor Sie Full Disk Encryption im Falle einer Beschädigung der Festplatte entfernen. • Die Reparatur-CD sollte nur dann verwendet werden, wenn die Standardmethoden zum Entfernen nicht durchführbar sind. Ein typisches Symptom einer beschädigten Festplatte ist ein schwarzer Bildschirm.

Full Disk Encryption Preboot Authentifizierung

Nach der Installation von Full Disk Encryption wird jetzt Full Disk Encryption Preboot vor dem Laden von Windows angezeigt. Full Disk Encryption Preboot spielt eine wichtige Rolle beim Sicherstellen, dass nur autorisierte Benutzer auf die Geräte zugreifen

können. Zudem werden bei einer Verbindung mit dem PolicyServer die lokalen Sicherheitsrichtlinien aktualisiert. Von diesem Fenster aus können Sie mehrere Aufgaben ausführen:

- Authentifizieren bei einem Endpunkt
- Kennwörter ändern
- Anmeldung an der Wiederherstellungskonsole



ABBILDUNG 5-1. Der Full Disk Encryption Preboot Bildschirm

Menüoptionen

Im oberen linken Menü von Full Disk Encryption Preboot stehen mehrere Optionen zur Verfügung.

TABELLE 5-2. Full Disk Encryption Preboot Menüoptionen

MENÜELEMENT	BESCHREIBUNG
Authentifizierung	Änderung der Authentifizierungsmethode, die bei der Anmeldung verwendet wird.
Kommunikation	Manuelle Synchronisierung mit PolicyServer. **Hinweis** Bei nicht verwalteten Endpunkten wird ein Null-Wert angezeigt.
Computer	Anzeige von Informationen über Full Disk Encryption, Ändern der Tastaturbelegung, Zugang zur Bildschirmtastatur oder Neustart bzw. Herunterfahren des Geräts.

Netzwerkverbindung

Wenn Full Disk Encryption als verwalteter Client installiert wurde, wird ein Netzwerkverbindungssymbol ( ) in der rechten oberen Ecke angezeigt. Dieses Symbol wird nur hervorgehoben, wenn das Gerät mit dem Netzwerk verbunden ist und eine Kommunikation mit dem PolicyServer stattfindet. Wenn Full Disk Encryption nicht verwaltet ist, wird das Netzwerksymbol nicht angezeigt.

Bildschirmtastatur

Greifen Sie auf die Bildschirmtastatur von Full Disk Encryption Preboot zu, indem Sie zu Folgenden navigieren:

Menu > **Computer** > **Bildschirmtastatur**

Um den Cursor in das gewünschte Feld zu setzen, wenn die Tastatur angezeigt wird, klicken Sie in der unteren rechten Ecke der Tastatur auf **Fokus**.

Tastaturbelegung ändern

Wird die Tastaturbelegung geändert, so wirkt sich dies sowohl auf Tastatureingaben als auch auf die Bildschirmtastatur aus. Nach dem Starten von Windows wird die Tastaturbelegung vom Windows-Betriebssystem festgelegt.

Prozedur

1. Navigieren Sie zu **Menü** > **Computer** > **Tastaturlayout ändern**.

   Das Fenster **Wählen Sie die Sprache für das Tastaturlayout aus** wird angezeigt.

2. Wählen Sie ein Tastaturlayout aus.

3. Klicken Sie auf **OK**.

Authentifizierungsmethode ändern

Prozedur

1. Wählen Sie in Full Disk Encryption Preboot die Option **Kennwort nach der Anmeldung ändern**.

2. Geben Sie den Benutzernamen und das Kennwort ein.

3. Klicken Sie auf **Anmelden**.

   Das Fenster **Kennwort ändern** wird angezeigt.

4. Wählen Sie aus dem Menü oben links **Authentifizierung** und wählen Sie die gewünschte Authentifizierungsmethode.

   Das Fenster **Neues Kennwort** der ausgewählten Authentifizierungsmethode wird angezeigt.

5. Geben Sie das neue Kennwort an, bestätigen Sie es, und klicken Sie anschließend auf **Weiter**.

Das Gerät startet Windows.

Kennwörter ändern

Prozedur

1. Wählen Sie in Full Disk Encryption Preboot die Option **Kennwort nach der Anmeldung ändern**.
2. Geben Sie den Benutzernamen und das Kennwort ein.
3. Klicken Sie auf **Anmelden**.

   Das Fenster **Kennwort ändern** wird angezeigt.
4. Geben Sie das neue Kennwort an, bestätigen Sie es, und klicken Sie anschließend auf **Weiter**.

   Das Gerät startet Windows.

ColorCode

ColorCode™ist eine einzigartige Authentifizierungsmethode, bei deren Entwicklung eine leichte Merkfähigkeit und schnelle Eingabe im Vordergrund standen. Anstelle der Verwendung von Ziffern und Buchstaben für ein Kennwort besteht die ColorCode-

Authentifizierung aus einer vom Benutzer erzeugten Farbfolge (z. B. rot, rot, blau, gelb, blau, grün).



ABBILDUNG 5-2. ColorCode-Anmeldung

ColorCode-Kennwort erstellen

Die Gesamtanzahl (Gesamtanzahl von Schritten in ColorCode) wird von PolicyServer definiert. Die Standardanzahl ist 6.

Prozedur

1. Ändern Sie die Authentifizierungsmethode in ColorCode.



Hinweis

Weitere Informationen über das Ändern von Authentifizierungsmethoden finden Sie unter *Authentifizierungsmethode ändern auf Seite 5-5*.

Das Fenster **ColorCode Kennwort ändern** wird angezeigt.

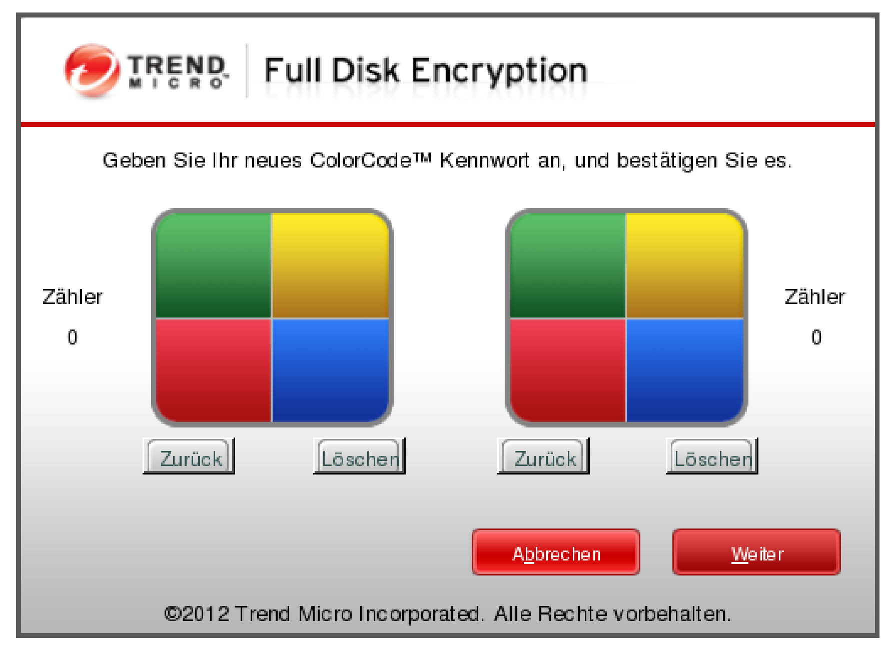


ABBILDUNG 5-3. Fenster "ColorCode Kennwort ändern"

2. Wählen Sie die erste Farbe, indem Sie im linken Quadrat darauf klicken.

   Die Anzahl erhöht sich um 1.

3. Klicken Sie auf die weiteren Farben in der Folge.



Tipp

Klicken Sie bei einem Fehler auf **Zurück**, um die zuletzt geklickte Farbe zu löschen, oder klicken Sie auf **Löschen**, um von neuem zu beginnen.

4. Wenn der Vorgang abgeschlossen ist, bestätigen Sie das ColorCode-Kennwort im rechten Quadrat.

5. Klicken Sie zum Abschluss auf **Weiter**.

Remote-Hilfe

Verwenden Sie die Remote-Hilfe, wenn der Zugriff eines Benutzers auf einen Endpunkt-Client gesperrt wurde, weil zu viele Anmeldeversuche fehlgeschlagen sind oder weil die Zeitspanne seit der letzten PolicyServer Synchronisierung zu lang ist.

Setzen Sie die Aktion in den Richtlinien jeder Anwendung auf **Remote-Authentifizierung**.

TABELLE 5-3. Richtlinien mit Auswirkungen auf die Authentifizierung für die Remote-Hilfe

RICHTLINIE	BESCHREIBUNG
Anmelden > **Zeitraum bis Kontosperrung**	Die Anzahl von Tagen, die ein Gerät ohne Kommunikation mit PolicyServer sein kann, bevor die Kontosperraktion ausgeführt wird.
Anmelden > **Kontosperraktion**	Die Aktion, die durchgeführt wird, wenn der angegebene Zeitraum abgelaufen ist. Mögliche Aktionen sind Löschen und Remote-Authentifizierung.
Anmelden > **Zulässige Anzahl fehlgeschlagener Anmeldeversuche**	Die Anzahl der zulässigen fehlgeschlagenen Anmeldeversuche, bevor die Aktion zur Gerätesperrung ausgeführt wird.
Anmelden > **Aktion zur Gerätesperrung**	Die Aktion, die durchgeführt wird, wenn der in der Richtlinie "Zulässige Anzahl fehlgeschlagener Anmeldeversuche" festgelegte Wert überschritten wurde. Mögliche Aktionen sind Zeitverzögerung, Löschen und Remote-Authentifizierung.

Remote-Hilfe zum Entsperren von Full Disk Encryption verwenden



Wichtig

- Durch einen Neustart des Endpunkt-Geräts wird der Herausforderungscode geändert.
- Durch eine manuelle Synchronisierung der Richtlinien mit PolicyServer wird der Herausforderungscode ebenfalls geändert.
- Bei Herausforderungscodes und Antwortcodes muss die Groß-/Kleinschreibung nicht berücksichtigt werden.

Prozedur

1. Wechseln Sie in Full Disk Encryption Preboot zu **Menü** > **Authentifizierung** > **Remote-Hilfe**.
2. Übergeben Sie den **Herausforderungscode** an den PolicyServer Administrator.
3. Geben Sie den **Antwortcode** ein, der vom PolicyServer Administrator bereitgestellt wird.
4. Klicken Sie auf **Anmelden**.

   Das Fenster **Kennwort ändern** wird angezeigt.

   Hinweis

   Wenn für das Konto die Domänenauthentifizierung verwendet wird, startet das Gerät direkt in Windows.

5. Geben Sie das neue Kennwort an, bestätigen Sie es und klicken Sie anschließend auf **Weiter**.

   Das Gerät startet Windows.

SmartCard

Die Smartcard-Authentifizierung erfordert sowohl eine PIN als auch eine physische Karte zur Bestätigung der Identität des Benutzers. Führen Sie die Smartcard vor der Eingabe der PIN ein.



Wichtig

Aktivieren Sie die folgende Richtlinie, um die Smartcard-Authentifizierung für alle Endpoint Encryption Clients zuzulassen: **Full Disk Encryption** > **PC** > **Anmelden** > **Token-Authentifizierung**.

Unterstützte Smartcards

KARTENHERSTELLER	PRODUKTNAME	LASERGRAVUR AUF KARTENRÜCKSEITE
Axalto	Axalto Cyberflex Access 64k v1 soft mask 4 Version 1	Axalto Access 64KV2
	Axalto Cyberflex Access 64k v1 soft mask 4 Version 2	Axalto Access 64KV2
Gemalto	Cyberflex Access v2c 64K	Gemalto Access 64KV2
	GemaltoGemCombiXpresso R4 dual interface	Gemalto GCX4 72K DI
	Gemalto TOP DL GX4 144K	Gemalto TOP DL GX4 144K
Gemplus	GemXpresso (GXP) PRO 64 K	Gemplus GXP3 64V2N
Oberthur	CosmopolIC v4 32K	Oberthur CosmopolIC v4
	Galactic v1 32K	OCS Gal 2.1
	ID-One Cosmo v5.2D 64k	Oberthur C.S. Cosmo64 V5.2D
	ID-One Cosmo v5.2 72k	Oberthur ID One V5.2
	ID-One Cosmo v5.2D 72k	Oberthur ID One V5.2 Dual

KARTENHERSTELLER	PRODUKTNAME	LASERGRAVUR AUF KARTENRÜCKSEITE
RSA	RSA 5100	
	RSA 5200	
	RSA 6100	
	RSA SID 800	
Schlumberger (Axalto)	Cyberflex 32k v2-Karte mit Softmask 7 Version 2	Schlumberger Access 32K V2

Authentifizierung mit einer Smartcard durchführen

Prozedur

1. Führen Sie die Smartcard in das Lesegerät ein.
2. Verbinden Sie das Lesegerät mit dem Gerät.
3. Geben Sie den Benutzernamen und das feste Kennwort ein.
4. Klicken Sie auf **Fortfahren**.

   Ein Meldungsfenster wird angezeigt.
5. Klicken Sie auf **Fortfahren**.
6. Im Fenster **Token registrieren**:
   a. Geben Sie die neue PIN ein, die Sie vom Administrator erhalten haben.
   b. Bestätigen Sie die neue PIN.
   c. Wählen Sie den Typ der Smartcard aus dem Listenfeld.
   d. Klicken Sie auf **Fortfahren**, um die Tokenregistrierung abzuschließen und auf den PC zuzugreifen.

Selbsthilfe

Benutzer verwenden die Selbsthilfe zur Authentifizierung, wenn sie ihre Anmeldedaten vergessen haben. Die Benutzer werden aufgefordert, die vordefinierten persönlichen Herausforderungsfragen der Selbsthilfe zu beantworten. Die Selbsthilfe kann anstelle von festen Kennwörtern oder anderen Authentifizierungsmethoden verwendet werden.



Wichtig

PolicyServer muss für die Selbsthilfe-Authentifizierung konfiguriert sein. Weitere Informationen finden Sie unter *Richtlinien verstehen auf Seite 3-1*.



Warnung!

Für Endpunkt-Clients können maximal sechs Fragen angezeigt werden. Erstellen Sie nicht mehr als sechs Fragen in PolicyServer, sonst können sich die Benutzer nicht anmelden.

Selbsthilfe einrichten

Wenn die Selbsthilfe-Richtlinie aktiviert ist, wird der Benutzer nach der ersten Anmeldung aufgefordert, Antworten auf diese Selbsthilfe-Fragen festzulegen. Wenn Benutzer ihr Kennwort ändern, müssen sie die Selbsthilfe-Fragen erneut festlegen.



Hinweis

Die Antworten zur Selbsthilfe werden auf dem Gerät gespeichert. Wenn ein Benutzer sich bei einem anderen Full Disk Encryption Gerät anmeldet, muss er Antworten für die Selbsthilfe für dieses Gerät festlegen.

Prozedur

1. Geben Sie den Benutzernamen und das Kennwort ein.
2. Klicken Sie auf **Anmelden**.

   Das Fenster **Selbsthilfe** wird angezeigt.
3. Legen Sie Antworten auf alle Selbsthilfe-Fragen fest.

4. Klicken Sie auf **Weiter**.

   Das Gerät startet Windows.

Selbsthilfe verwenden

Prozedur

1. Wechseln Sie im oberen linken Menü von Full Disk Encryption Preboot zu **Menü** > **Authentifizierung** > **Selbsthilfe**.

   Das Fenster **Selbsthilfe** wird angezeigt.

2. Beantworten Sie alle Fragen zur Selbsthilfe.

3. Klicken Sie auf **Anmelden**.

4. Legen Sie ein neues Kennwort fest und klicken Sie anschließend auf **Weiter**.

   Das Gerät startet Windows.

Antworten für die Selbsthilfe ändern

Prozedur

1. Geben Sie in Full Disk Encryption Preboot Ihre Anmeldedaten ein, wählen Sie **Kennwort nach der Anmeldung ändern** und klicken Sie anschließend auf **Anmelden**.

   Das Fenster **Kennwort ändern** wird angezeigt.

2. Geben Sie das neue Kennwort an, bestätigen Sie es, und klicken Sie anschließend auf **Weiter**.

   Das Fenster **Selbsthilfe** wird angezeigt.

3. Legen Sie neue Antworten auf alle Selbsthilfe-Fragen fest und klicken Sie anschließend auf **Weiter**.

Das Gerät startet Windows.

Full Disk Encryption Konnektivität

Endpoint Encryption verwendet einen zugelassenen FIPS 140-2-Verschlüsselungsprozess für Daten, die zwischen Full Disk Encryption Preboot und PolicyServer übertragen werden. Full Disk Encryption Clients haben eine Netzwerkverbindung zum PolicyServer und können Richtlinien-Updates empfangen und Audit-Daten vom Endpunktclient hochladen. Die gesamte Client-Server-Kommunikation wird intern verschlüsselt und kann über ungesicherte Verbindungen wie das Internet gesendet werden.

Systemadministratoren erhalten Flexibilität beim Festlegen der Verbindungsmöglichkeiten für ihr Unternehmen. Administratoren können den PolicyServer innerhalb einer DMZ (Demilitarisierte Zone) platzieren, um ihn sowohl für interne Netzwerke als auch das Internet zugänglich zu machen.

TABELLE 5-4. Full Disk Encryption Konnektivitätsanforderungen

RESSOURCE	FUNKTION
PolicyServer	Aktualisierte Sicherheitsrichtlinien vom PolicyServer können an Full Disk Encryption Preboot oder mit Hilfe von Verbindungen innerhalb von Windows, LAN, VPN usw. gesendet werden.
TCP/IP-Zugriff	Netzwerkverbindungen für PCs erfordern vollen TCP/IP-Netzwerkzugriff. DFÜ- oder Telefonzugriff kann nicht zur Bereitstellung der Verbindung mit dem PolicyServer während der Preboot-Authentifizierung verwendet werden.
Port 80	Die Full Disk Encryption Kommunikation verwendet standardmäßig Port 80. Um die Standardportnummer zu ändern, navigieren Sie zur Wiederherstellungskonsole und aktualisieren Sie den PolicyServer.

Aktualisieren von Full Disk Encryption Clients

Full Disk Encryption Clients erhalten automatisch aktualisierte Sicherheitsrichtlinien vom PolicyServer in Intervallen, die von der Richtlinie vorgegeben werden. Gehen Sie wie folgt vor, um Richtlinien manuell zu synchronisieren:

Prozedur

1. Navigieren Sie im oberen linken Menü von Full Disk Encryption Preboot zu **Kommunikation** > **Synchronisierung von Richtlinien**.
2. Navigieren Sie zu **Computer** > **Info über Full Disk Encryption**. Der Zeitstempel der aktuellsten PolicyServer Richtliniensynchronisierung wird angezeigt.

Full Disk Encryption – Wiederherstellungskonsole

Mit der Wiederherstellungskonsole können Administratoren ein Gerät beim Ausfall des primären Betriebssystems wiederherstellen, Probleme mit der Netzwerkverbindung lösen und Richtlinien für nicht verwaltete Clients verwalten.



Warnung!

Verwenden Sie die Wiederherstellungskonsole vor dem Ausführen der Standard-Diagnose- und Reparaturprogramme von Windows.

TABELLE 5-5. Funktionen der Wiederherstellungskonsole

KONSOLENELEMENT	BESCHREIBUNG
Festplatte entschlüsseln	Verschlüsselung von der Festplatte entfernen. Verwenden Sie die Full Disk Encryption Preboot-Wiederherstellungskonsole, um auf die Option "Festplatte entschlüsseln" zuzugreifen.

KONSOLENELEMENT	BESCHREIBUNG
Partitionen bereitstellen	Bereitstellung von Zugriff auf die verschlüsselten Partitionen zur Dateiverwaltung. Verwenden Sie die Full Disk Encryption Preboot-Wiederherstellungskonsole, um auf die Option "Partitionen bereitstellen" zuzugreifen. **Hinweis** Auf "Partitionen bereitstellen" kann nur von Geräten mit Softwareverschlüsselung aus zugegriffen werden. Diese Option ist abgeblendet, wenn ein Gerät über Hardware-Verschlüsselung verfügt.
Bootsektor wiederherstellen	Rollback des MBR zu einem Zustand vor der Installation von Full Disk Encryption. Verwenden Sie die Full Disk Encryption Preboot-Wiederherstellungskonsole, um auf die Option "Bootsektor wiederherstellen" zuzugreifen. **Hinweis** Auf "Bootsektor wiederherstellen" kann nur von Geräten mit Softwareverschlüsselung aus zugegriffen werden. Diese Option ist abgeblendet, wenn ein Gerät über Hardware-Verschlüsselung verfügt.
Benutzer verwalten	Hinzufügen oder Entfernen von Benutzern von einem Gerät, wenn es nicht mit dem PolicyServer verbunden ist.
Richtlinien verwalten	Ändern Sie die Richtlinien für Geräte, die entweder nicht von PolicyServer verwaltet werden oder die verwaltet werden, aber die vorübergehend nicht mit PolicyServer verbunden sind. Wenn das Gerät verwaltet ist, werden Richtlinienänderungen bei der nächsten Kommunikation des Geräts mit PolicyServer überschrieben.
Protokolle anzeigen	Anzeigen und Durchsuchen verschiedener Full Disk Encryption Protokolle. **Hinweis** Protokolle sind nur verfügbar, wenn von Windows aus auf die Wiederherstellungskonsole zugegriffen wird.

KONSOLENELEMENT	BESCHREIBUNG
Netzwerk-Setup	Überprüfen, Testen und Ändern von Netzwerkeinstellungen.
Beenden	Beenden der Wiederherstellungskonsole.

Auf die Wiederherstellungskonsole zugreifen

Nur Gruppenadministrator- und Authentifiziererkonten können auf die Wiederherstellungskonsole zugreifen. Um Benutzern Zugriff auf die Wiederherstellungskonsole zu geben, setzen Sie **PC** > **Client** > **Wiederherstellung durch Benutzer zulassen** auf **Ja**.

Prozedur

1. Starten Sie das Gerät neu.
2. Wenn "Full Disk Encryption Preboot" angezeigt wird, geben Sie den Benutzernamen und das Kennwort ein.
3. Wählen Sie die Option **Wiederherstellungskonsole** und melden Sie sich dann an.

   Die Wiederherstellungskonsole wird angezeigt.

Auf die Wiederherstellungskonsole von Windows aus zugreifen

Prozedur

1. Wechseln Sie unter Windows zum Installationsverzeichnis von Full Disk Encryption. Der Standardordner ist `C:\Programme\Trend Micro\Full Disk Encryption\`
2. Öffnen Sie `RecoveryConsole.exe`.

   Das Fenster **Wiederherstellungskonsole** wird angezeigt.

3. Geben Sie Ihren Benutzernamen und das Kennwort ein und klicken Sie dann auf **Anmelden**.

   Die Wiederherstellungskonsole wird mit der Seite **Festplatte entschlüsseln** geöffnet.

"Festplatte entschlüsseln" verwenden

Durch Auswählen von "Festplatte entschlüsseln" wird eine verschlüsselte Full Disk Encryption Festplatte entschlüsselt, aber die Treiber für die Verschlüsselung werden nicht entfernt. Wenn Sie "Festplatte entschlüsseln" verwenden, deaktivieren Sie DrAService, bevor Sie Windows starten.



Warnung!

Lesen Sie die Anweisungen zu diesem Verfahren, bevor Sie "Festplatte entschlüsseln" verwenden. Bei falscher Vorgehensweise kann der Verlust von Daten nicht ausgeschlossen werden. Entfernen Sie Full Disk Encryption nicht mit Hilfe von "Festplatte entschlüsseln", wenn das Gerät normal funktioniert. Verwenden Sie stattdessen `TMFDEUninstall.exe`.

Prozedur

1. Wählen Sie in Full Disk Encryption Preboot die Option **Wiederherstellungskonsole** aus, geben Sie Anmeldedaten ein und klicken Sie dann auf **Anmelden**.

   Die Wiederherstellungskonsole wird mit der Seite **Festplatte entschlüsseln** geöffnet.

2. Klicken Sie auf **Entschlüsseln**, um mit der Entschlüsselung des Laufwerks zu beginnen.

   Mit der Entschlüsselung wird direkt begonnen, und es wird die Seite "Festplatte entschlüsseln" mit dem Entschlüsselungsfortschritt angezeigt.

3. Klicken Sie nach Beendigung der Entschlüsselung auf **Beenden**, um das Gerät neu zu starten.

4. Beim Starten mit einer CD, DVD oder einem USB-Dongle mit einem Reparaturtool:

   a. Nach der Beendigung von Full Disk Encryption drücken Sie **F12** (oder die entsprechende Taste, um zu den Boot-Optionen zu gelangen).

   b. Legen Sie die CD/DVD mit dem Reparaturtool ein, und wählen Sie im Fenster mit den Boot-Optionen "CD/DVD-Laufwerk".

   c. Fahren Sie mit den etablierten Wiederherstellungsmaßnahmen fort.

5. Beim Starten von Windows:

   a. Halten Sie F8 gedrückt, und wählen Sie **Abgesicherter Modus**, bevor das System beginnt, Windows zu starten.



Warnung!

Wenn Sie das Fenster mit den Windows Boot-Optionen verpassen, schalten Sie das Gerät sofort aus. Wenn Windows normal gestartet wird (nicht im abgesicherten Modus), wird DrAService sofort damit beginnen, die Festplatte erneut zu verschlüsseln. Bei allen Wiederherstellungsmaßnahmen, die an diesem Punkt durchgeführt werden, besteht das Risiko, dass die Daten auf der Festplatte irreparabel beschädigt werden.

---

6. Öffnen Sie **Geräteverwaltung** und navigieren Sie zu **Dienste und Anwendungen** > **Dienste.**

Das Fenster **Geräteverwaltung** wird angezeigt.

7. Machen Sie DrAService ausfindig und doppelklicken Sie darauf, um das Fenster **Eigenschaften von DrAService** anzuzeigen.

8. Ändern Sie auf der Registerkarte **Allgemein** den **Starttyp** in `Deaktiviert`.

9. Klicken Sie auf **Übernehmen**, und klicken Sie anschließend auf **OK**.

10. Starten Sie das Gerät neu.

11. Melden Sie sich erst bei Full Disk Encryption Preboot an und dann bei Windows.

Nächste Maßnahme

Nach dem Abschluss aller Wiederherstellungsaktionen legen Sie für **DrAService** den Starttyp **Automatisch** fest. Das Geräte verschlüsselt die Festplatte nach dem nächsten Neustart automatisch erneut.

Partitionen bereitstellen

Kopieren Sie mit Hilfe von "Partitionen bereitstellen" Dateien zwischen der verschlüsselten Festplatte und einem Speichergerät, bevor Sie ein Image der Festplatte erstellen oder diese neu formatieren. Der verschlüsselte Inhalt auf dem Laufwerk wird im linken Fensterbereich angezeigt, und das unverschlüsselte Gerät kann im rechten Fensterbereich gemountet werden. Verschieben Sie Dateien mit Kopieren und Einfügen zwischen den Fensterbereichen. Dateien, die auf das verschlüsselte Laufwerk kopiert werden, werden verschlüsselt. Bei Dateien, die vom verschlüsselten Laufwerk kopiert werden, wird die Verschlüsselung aufgehoben.

Bootsektor wiederherstellen

Mit Hilfe der Option "Bootsektor wiederherstellen" wird der ursprüngliche Bootsektor des Geräts wiederhergestellt, wenn das Gerät vollständig entschlüsselt ist. Diese Option ist nur in Full Disk Encryption Preboot verfügbar.

Entschlüsseln Sie die Festplatte, bevor Sie den Master Boot Record (MBR) wiederherstellen.



Warnung!

Sie sollten jedoch "Festplatte entschlüsseln" nicht aufrufen, bevor Sie die Anweisungen gelesen haben. Datenverluste können auftreten.

Prozedur

1. Melden Sie sich bei der Wiederherstellungskonsole an.
2. Klicken Sie auf **Festplatte entschlüsseln** und klicken Sie dann auf **Entschlüsseln**.

3. Wechseln Sie zur Option "Bootsektor wiederherstellen".

   Das Bestätigungsfenster **Möchten Sie den MBR wirklich ersetzen?** wird angezeigt.

4. Klicken Sie auf **Ja**, um den MBR zu ersetzen.

   Eine Nachricht mit der Bestätigung, dass der MBR ersetzt wurde, wird angezeigt.

5. Klicken Sie auf **Beenden**.

   Das Gerät startet Windows.

Full Disk Encryption Benutzer verwalten

Sie können Benutzer dem Preboot-Cache hinzufügen bzw. daraus entfernen oder das im Cache gespeicherte Kennwort des Benutzers ändern. Diese Option ist nützlich, wenn Full Disk Encryption keine Verbindung zu PolicyServer aufbauen kann. Diese Option kann sowohl von Full Disk Encryption Preboot als auch von der Windows Wiederherstellungskonsole verwendet werden.



Hinweis

- "Benutzer verwalten" ist nur verfügbar, wenn keine Verbindung mit PolicyServer besteht.
- Änderungen, die an Benutzern vorgenommen wurden, werden überschrieben, wenn Full Disk Encryption eine Verbindung zu PolicyServer aufbaut.

Einige Überlegungen zu Kennwörtern:

- Die zugewiesenen Kennwörter, ob für ein neues oder bestehendes Konto, sind feste Kennwörter.
- Das Ablaufdatum für Benutzerkennwörter kann direkt über den Kalender "Kennwort läuft ab" festgelegt werden.
- Die Standardeinstellung für einen neuen Benutzer ist das Datum, das durch die Richtlinie "Kennwort ändern alle" festgelegt wird. Diese Richtlinie befindet sich unter: **Allgemein** > **Authentifizierung** > **Benutzerkennwort**.



Hinweis

Wenn Sie für das Datum das aktuelle oder ein älteres Datum festlegen, wird eine direkte Kennwortänderung erzwungen, während die Festlegung auf ein zukünftiges Datum eine Änderung an diesem Datum festlegt.

Benutzer bearbeiten

Beim Bearbeiten eines Benutzers in der Wiederherstellungskonsole gelten die gleichen Regeln wie in PolicyServer. Weitere Informationen zu Regeln finden Sie unter *Benutzer zu PolicyServer hinzufügen auf Seite 4-10*.

Prozedur

1. Wählen Sie den Benutzer aus der Benutzerliste aus.
2. Aktualisieren Sie die gewünschten Informationen.
3. Wählen Sie den Benutzertyp aus: Administrator, Authentifizierer oder Benutzer.
4. Legen Sie das Ablaufdatum für das Kennwort fest.
5. Klicken Sie auf **Speichern**.

   Der Benutzer wird aktualisiert.

Benutzer hinzufügen

Prozedur

1. Klicken Sie auf **Benutzer hinzufügen**.
2. Geben Sie Ihren Benutzernamen und das Kennwort ein, und bestätigen Sie das Kennwort.
3. Wählen Sie die Authentifizierungsmethode aus der Dropdown-Liste **Authentifizierungstyp**.
4. Legen Sie das Ablaufdatum für das Kennwort fest.

5. Klicken Sie auf **Speichern**.

   Der neue Benutzer wird in der Benutzerliste angezeigt. Eine Bestätigungsmeldung wird angezeigt.

6. Klicken Sie auf **OK**, um das Bestätigungsfenster zu schließen.

   Der neue Benutzer wird hinzugefügt.

Benutzer löschen

Prozedur

1. Wählen Sie einen Benutzer aus der Benutzerliste aus.

2. Klicken Sie auf **Benutzer löschen**.

   Ein Bestätigungsfenster zum Löschen des Benutzers wird angezeigt.

3. Klicken Sie auf **Ja**.

   Der Benutzer wird aus der Benutzerliste gelöscht.

Richtlinien verwalten

Verwenden Sie "Richtlinien verwalten", um die verschiedenen Richtlinien für die Full Disk Encryption Wiederherstellungskonsole festzulegen. Eine Erklärung dieser Richtlinien finden Sie unter *Richtlinien verstehen auf Seite 3-1*.



Hinweis

Die Option "Richtlinien verwalten" ist nur verfügbar, wenn keine Verbindung mit dem PolicyServer besteht. Die vorgenommenen Änderungen werden überschrieben, wenn Full Disk Encryption das nächste Mal eine Verbindung zu PolicyServer aufbaut.

Protokolle anzeigen

Mit dem Befehl "Protokolle anzeigen" können Administratoren Protokollen suchen und sie auf Grundlage spezifischer Kriterien anzeigen. "Protokolle anzeigen" ist nur in der Wiederherstellungskonsole unter Windows verfügbar. Der Befehl ist über Full Disk Encryption Preboot nicht verfügbar.

Informationen über das Anzeigen von Full Disk Encryption Protokollen finden Sie unter *Auf die Wiederherstellungskonsole von Windows aus zugreifen auf Seite 5-18*.

Netzwerk-Setup

Das Netzwerk-Setup wird zum Überprüfen, Testen und/oder Ändern der Netzwerkeinstellungen von Full Disk Encryption Preboot verwendet. Es stehen drei Registerkarten zur Verfügung: **IPv4**, **IPv6** und **PolicyServer**.



Hinweis

Neu in Full Disk Encryption 3.1.3 ist die Fähigkeit, PolicyServer oder das Unternehmen zu wechseln, ohne Full Disk Encryption entfernen und neu installieren zu müssen.

Netzwerkkonfiguration verwalten

Standardmäßig ist **Einstellungen von Windows abrufen** für IPv4 und IPv6 ausgewählt. Deaktivieren Sie diese Option, um die Netzwerkeinstellungen manuell zu konfigurieren.

- Die Auswahl von **DHCP** (IPv4) oder **Adresse automatisch abrufen** (IPv6) verwendet die dynamisch zugewiesene IP-Adresse.
- Bei Auswahl von **Statische IP-Adresse** werden alle Felder in diesem Abschnitt aktiviert.
- Wenn Sie auf der Registerkarte **IPv6** die Option **Statische IP-Adresse** auswählen und das Feld "IP-Adresse" leer ist, wird eine eindeutige IP-Adresse auf Grundlage der Hardware-Adresse des Computers erzeugt.

PolicyServer Einstellungen verwalten

Prozedur

1. Öffnen Sie die Registerkarte **PolicyServer**. Die Registerkarte enthält zwei Textfelder: **Aktueller Server** und **Aktuelles Unternehmen**.

   - Das aktuelle Unternehmen wechseln:

     a. Klicken Sie auf **Unternehmen wechseln**.

     b. Klicken Sie auf **Ja**, wenn die Warnmeldung angezeigt wird.

     c. Geben Sie den Benutzernamen, das Kennwort, das Unternehmen und den Servernamen für den neuen Server ein und klicken Sie anschließend auf **Speichern**.

     Warnung!

     Wenn Sie das Unternehmen wechseln, müssen Sie die Richtlinien erneut konfigurieren und die Gruppen neu erstellen. Die gespeicherten Kennwörter, der Kennwortverlauf und die Audit-Protokolle werden gelöscht.

   - Den aktuellen Server wechseln:

     a. Klicken Sie auf **Server wechseln**.

     b. Klicken Sie auf **Ja**, wenn die Warnmeldung angezeigt wird.

     c. Geben Sie die Adresse des neuen Servers ein und klicken Sie auf **Speichern**.

2. Klicken Sie auf **Abbrechen**, um zum Fenster mit den Menüoptionen für die Wiederherstellungskonsole zurückzukehren.

Full Disk Encryption Wiederherstellungsmethoden

Sobald ein Gerät mit Full Disk Encryption vollständig verschlüsselt ist, können Szenarios eintreten, in denen ein Administrator mehrere Systemwiederherstellungsaktionen durchführen muss:

- Das lokale Administratorkennwort wurde vergessen
- Die Windows-Umgebung ist beschädigt



Wichtig

Bei einer Softwareverschlüsselung können herkömmliche Tools zur Datenwiederherstellung (z. B. Windows Recovery Disk, ERD Commander, UBCD) nicht auf ein mit Full Disk Encryption 3.1.3 verschlüsseltes System zugreifen. Deshalb muss das System entschlüsselt werden, bevor Maßnahmen zur Wiederherstellung durchgeführt werden.

Die Methoden zur Datenwiederherstellung sind für Endpoint Encryption Administratoren/Authentifizierer verfügbar, um Daten wiederherzustellen, wenn das Gerät nicht ordnungsgemäß funktioniert. Full Disk Encryption muss installiert sein.

Tabelle 5-6. Wiederherstellungsfunktionen für Full Disk Encryption-geschützte Geräte

Wiederherstellungs methode	Beschreibung	Wann verwenden
Deinstallation von Full Disk Encryption	Bei der Deinstallation von Full Disk Encryption wird Full Disk Encryption vom Gerät entfernt. Nachdem die Deinstallation abgeschlossen ist, können Sie unter Windows mit etablierten Wiederherstellungsmaßnahmen fortfahren.	Windows-Umgebung arbeitet normal.

Wiederherstellungsmethode	Beschreibung	Wann verwenden
Wiederherstellungskonsole	Bei Auswahl der Option Full Disk Encryption **Wiederherstellungskonsole** > **Festplatte entschlüsseln** können Administratoren die ausgewählte Festplatte direkt entschlüsseln oder das Image der entschlüsselten Festplatte auf einem Wechseldatenträger speichern. **Hinweis** Diese Methode sollte nicht ausgeführt werden, wenn Windows normal funktioniert.	Wenn Full Disk Encryption Preboot geladen wird, Windows jedoch nicht.
Reparatur-CD	Bei der Reparatur-CD handelt es sich um eine bootfähige CD, mit deren Hilfe ein beschädigtes Laufwerk entschlüsselt wird, wenn das Gerät nicht mit Full Disk Encryption hochgefahren werden kann. Ein typisches Symptom einer beschädigten Festplatte ist ein schwarzer Bildschirm. **Warnung!** Nicht verwenden, wenn Windows normal funktioniert.	• Full Disk Encryption Preboot wird nicht geladen. • Full Disk Encryption kann nicht authentifiziert werden.



Hinweis

Damit das Laufwerk entschlüsselt werden kann, muss es sich beim Benutzer um einen Endpoint Encryption Unternehmens- oder Gruppenadministrator mit Administratorrechten unter Windows handeln.

Reparatur-CD

Bei der Full Disk Encryption Reparatur-CD handelt es sich um eine bootfähige CD, mit deren Hilfe ein Gerät vollständig entschlüsselt werden kann, wenn das Gerät nicht mehr in der Lage ist, gestartet zu werden.



Hinweis

- Wenn auf der Festplatte physische Schäden (beschädigte Sektoren) aufgetreten sind, kann das Laufwerk möglicherweise nicht vollständig entschlüsselt werden oder wird u. U. unbrauchbar.
- Überprüfen Sie, ob das Festplattenkabel ordnungsgemäß angeschlossen ist.

Nach dem Booten von der Reparatur-CD sind mehrere Optionen verfügbar:

TABELLE 5-7. Optionen der Reparatur-CD

OPTIONEN	BESCHREIBUNG
Wiederherstellung	Startet die Wiederherstellungskonsole.
Entsperren	Entsperrt ein Gerät, das aus folgenden Gründen gesperrt wurde: • Es sind viele erfolglose Anmeldeversuche erfolgt. • Keine Kommunikation mit PolicyServer für eine bestimmte Dauer **Hinweis** Die Option zum Entsperren ist nur verfügbar, wenn die Richtlinien-Remote-Authentifizierung auf **Abmelden** festgelegt ist.

Optionen	Beschreibung
Neu starten	Startet das Gerät neu.
Erweiterte Optionen	Bietet Zugriff auf erweiterte Optionen: • Full Disk Encryption Preboot entfernen • Löschen • Entschlüsselung erzwingen

Tabelle 5-8. Erweiterte Optionen der Reparatur-CD

Erweiterte Option	Beschreibung
Full Disk Encryption Preboot entfernen	Entfernt das Full Disk Encryption Preboot Authentifizierungsfenster vom Gerät. **Warnung!** Diese Aktion kann nicht rückgängig gemacht werden. Dabei wird das Laufwerk nicht entschlüsselt. Entfernen Sie die Verschlüsselung mit der Option "Festplatte entschlüsseln".
Löschen	Entfernt alle Daten vom Gerät.
Zurück zum Hauptmenü	Kehrt zu den Standard-CD-Optionen zurück.
Entschlüsselung erzwingen	Ermöglicht einem Administrator, das Laufwerk zu entschlüsseln, wenn Full Disk Encryption nicht gestartet werden kann.



Warnung!

Bei falscher Anwendung der erweiterten Optionen besteht das Risiko von Datenverlusten.

Daten mit der Reparatur-CD wiederherstellen

Mit der Reparatur-CD können Sie versuchen, Daten von einem verschlüsselten Laufwerk wiederherzustellen. Es gibt jedoch mehrere Überlegungen, die Sie beachten sollten, bevor Sie versuchen, die Festplatte zu entschlüsseln:

- Verwenden Sie die Reparatur-CD nur dann, wenn das Gerät verschlüsselt ist oder mit der Verschlüsselung begonnen wurde.
- Wenn das Gerät wichtige Daten enthält, fertigen Sie eine Sicherheitskopie an, bevor Sie fortfahren. Anweisungen finden Sie unter http://esupport.trendmicro.com/solution/en-us/1059802.aspx.
- Versuchen Sie nicht, die Festplatte in einem Laptop zu entschlüsseln, es sei denn, er ist an das Stromnetz angeschlossen.
- Wenn die Reparatur-CD nicht gebootet wird, überprüfen Sie, ob auf dem Gerät die neueste BIOS-Version installiert ist. Aktualisieren Sie ggf. das System-BIOS.
- Die Laufwerksentschlüsselung mit dieser Methode dauert mindestens so lange wie die anfängliche Verschlüsselung.
- Wenn ein fehlerhafter Sektor gefunden wird, wird der Prozess deutlich verlangsamt. Führen Sie die Entschlüsselung weiter mit der CD aus, und wenden Sie sich an den Support von Trend Micro, bevor Sie den Prozess unterbrechen.



Warnung!

Unterbrechen Sie den Prozess nicht, nachdem Sie die Entschlüsselung von der CD eingeleitet haben, da es sonst zu irreversiblen Datenverlusten kommen kann.

Festplatte mit der Reparatur-CD entschlüsseln

Prozedur

1. Schalten Sie das vernetzte System ein.

   a. Drücken Sie sofort **F12** (oder die entsprechende Taste, um zu den Boot-Optionen zu gelangen).

   b. Legen Sie die Reparatur-CD ein, und wählen Sie im Fenster mit den Boot-Optionen "CD/DVD-Laufwerk".

      Das Gerät bootet und lädt die Umgebung der Reparatur-CD.

2. Wählen Sie bei Full Disk Encryption Preboot die Option **Wiederherstellungskonsole**.

3. Geben Sie den Benutzernamen und das Kennwort ein.

4. Klicken Sie auf **Anmelden**.

   Die Wiederherstellungskonsole wird angezeigt.

5. Wählen Sie **Festplatte entschlüsseln**, um mit der Entschlüsselung des Laufwerks zu beginnen.

6. Wenn die Entschlüsselung abgeschlossen ist, klicken Sie auf **Beenden**, um zum Menü der Reparatur-CD zurückzukehren.

7. Klicken Sie auf **Neu starten**, um das Gerät neu zu starten.



Hinweis

Entfernen Sie die CD, um das Gerät manuell zu starten.

8. Melden Sie sich bei Full Disk Encryption Preboot an.

9. Melden Sie sich bei Windows an und fahren Sie mit der bevorzugten Wiederherstellungsmethode fort.

Full Disk Encryption Dateien entfernen

Beim Entschlüsseln eines Laufwerks werden MBR-Änderungen und andere wichtige für den Schutz des Geräts verwendeten Elemente entfernt. Wenn Sie Software verschlüsseln, entschlüsseln Sie die Festplatte vollständig, bevor Sie Full Disk Encryption deinstallieren. Andernfalls stürzt das Betriebssystem möglicherweise ab.



Warnung!

Wenn Sie MSI azf eunen nicht-DriveTrust-Computer deinstallieren, wird das Betriebssystem erst nach dem Neustart des Client gefunden.

Prozedur

1. Gehen Sie an einer Befehlszeile wie folgt vor:

   a. Führen Sie `msiexec.exe /X{17BACE08-76BD-4FF5-9A06-5F2FA9EBDDEA}` aus.

2. Aus Windows:

   a. Starten Sie **`regedit`** aus Windows heraus, und navigieren Sie zu folgendem Schlüssel: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\\{17BACE08-76BD-4FF5-9A06-5F2FA9EBDDEA}`.

   b. Navigieren Sie zum Schlüssel `UninstallString`: `msiexec.exe /x {17BACE08-76BD-4FF5-9A06-5F2FA9EBDDEA}`.

   c. Kopieren Sie die Zeichenfolge.

   d. Öffnen Sie den Befehl **Ausführen...** und fügen Sie die Zeichenfolge in das Textfeld **Öffnen** ein.

   e. Klicken Sie auf **OK**.

   Das Fenster **Windows Installer** wird angezeigt.

   f. Wenn die Deinstallationsbestätigung angezeigt wird, klicken Sie auf **Ja**.



Hinweis

Wenn das Fenster **Benutzerkontensteuerung** angezeigt wird, klicken Sie auf **Zulassen**.

   g. Wenn Sie aufgefordert werden, den DrAService zu beenden, wählen Sie das zweite Optionsfeld **Anwendungen nicht schließen** und klicken Sie anschließend auf **OK**.

3. Wenn Sie dazu aufgefordert werden, das Gerät neu zu starten, klicken Sie auf **Ja**. Starten Sie andernfalls das Gerät manuell neu.



Kapitel 6

Mit FileArmor arbeiten

FileArmor schützt einzelne Dateien und Ordner auf lokalen Festplatten und auf Wechselmedien (USB-Laufwerken). Administratoren können Richtlinien festlegen, die angeben, welche Ordner und Laufwerke auf dem Gerät verschlüsselt sind, und die Richtlinien zu verschlüsselten Daten auf Wechselmedien festlegen. Verschlüsselung wird durchgeführt, nachdem die Authentifizierung stattgefunden hat.

FileArmor kann auch verschiedene Dateien mit unterschiedlichen Schlüsseln schützen, was Administratoren ermöglicht, Zugriffsrichtlinien für ein Gerät und separate Richtlinien für den Zugriff auf bestimmte Dateien festzulegen. Dies ist in Umgebungen nützlich, in denen mehrere Benutzer auf einen Endpunkt zugreifen.

Dieses Kapitel umfasst folgende Themen:

- *FileArmor Task-Leistensymbolmenü auf Seite 6-8*
- *FileArmor Authentifizierung auf Seite 6-2*
- *FileArmor Verschlüsselung auf Seite 6-11*
- *FileArmor Sicheres Löschen auf Seite 6-17*

FileArmor Authentifizierung

In diesem Abschnitt wird beschrieben, wie die Authentifizierung mit FileArmor durchgeführt wird. Darüber hinaus werden weitere Aspekte der Verwendung von FileArmor erläutert. Alle Authentifizierungsmethoden für Endpoint Encryption sind in FileArmor verfügbar. Weitere Informationen zu Authentifizierungsmethoden finden Sie unter *Kontenrollen und Authentifizierung auf Seite 1-13*.

Erste Authentifizierung bei FileArmor

Wenn FileArmor zum ersten Mal gestartet wird, ist eine Authentifizierung erforderlich, um PolicyServer zu identifizieren. Die Standardmethode ist die Authentifizierung mit festem Kennwort. Weitere Optionen hängen von den Richtlinieneinstellungen ab.

Prozedur

1. Klicken Sie mit der rechten Maustaste auf das FileArmor Symbol in der Task-Leiste, und wählen Sie **Registrieren**.
2. Geben Sie den Benutzernamen und das Kennwort ein.
3. Geben Sie die IP-Adresse (oder den Host-Namen) sowie das Unternehmen des PolicyServer ein.
4. Klicken Sie auf **OK**.

   Das Fenster **Kennwort ändern** wird angezeigt.
5. Wählen Sie die gewünschte Authentifizierung aus dem Listenfeld aus.
6. Geben Sie das neue Kennwort an, bestätigen Sie es und klicken Sie anschließend auf **OK**.



Hinweis

Ohne Authentifizierung bei FileArmor wird der Zugriff auf Dateien und Wechselmedien verweigert.

FileArmor Domänenauthentifizierung

Zur nahtlosen Integration und Verwendung des FileArmor Prozesses zur Domänenauthentifizierung/Single-Sign-On (SSO) vergewissern Sie sich, dass die folgenden Anforderungen erfüllt werden:

- Der Benutzer gehört einer Gruppe an, bei der die Richtlinie **Allgemein** > **Authentifizierung** > **Domänenauthentifizierung** auf **Ja** eingestellt ist.
- Wechseln Sie auf Gruppenebene zu **Allgemein** > **Authentifizierung** > **Netzwerkanmeldung** und legen Sie den Host-Namen und den Domänennamen fest.
- PolicyServer und alle Geräte, die die Domänenauthentifizierung verwenden, befinden sich in derselben Domäne.
- Das Benutzerkonto wird in Active Directory und PolicyServer konfiguriert. Der Benutzername muss genau übereinstimmen, auch hinsichtlich der Groß- und Kleinschreibung.



Hinweis

Für FileArmor SSO muss die folgende Richtlinie aktiviert sein: **Allgemein** > **Authentifizierung** > **Netzwerkanmeldung** > **Domänenauthentifizierung**.

Authentifizierung mit Domänenauthentifizierung durchführen

Aktivieren Sie die Domänenauthentifizierung unter:

Gruppenname > **Richtlinien** > **Allgemein** > **Authentifizierung** > **Netzwerkanmeldung** > **Domänenauthentifizierung**.

Prozedur

1. Wählen Sie **Domänenauthentifizierung** als Authentifizierungstyp.
2. Geben Sie den Benutzernamen und das Kennwort für das Domänenkonto ein.

3. Klicken Sie auf **OK**.



Hinweis

- Für Domänenbenutzer ist das Ändern von Kennwörtern nicht verfügbar und mit FileArmor kann ein Windows Domänenkennwort nicht geändert werden. Diese Funktionalität wird durch Active Directory gesteuert.
- Die Domänenauthentifizierung kann nicht mit einer Smartcard-PIN verwendet werden.
- Die Remote-Hilfe ist für Domänenbenutzer verfügbar. Das Domänenkennwort muss allerdings in Active Directory zurückgesetzt werden, wenn es vergessen wird.

FileArmor Smartcard-Authentifizierung

Stellen Sie zur Verwendung der Smartcard-Authentifizierung sicher, dass die folgenden Anforderungen erfüllt werden:

- FileArmor Richtlinie **Anmelden** > **Kennwort** > **Physischer Token erforderlich** = **Ja**.
- Das Smartcard-Lesegerät ist verbunden und die Smartcard ist eingelegt.



Hinweis

FileArmor unterstützt nur CASC- und PIC-Smartcards.

- ActivClient 6.1 muss mit allen Service Packs und Updates installiert sein.
- Geben Sie die Smartcard-PIN in das Kennwortfeld ein.



Warnung!

Wenn kein gültiges Kennwort eingegeben wird, wird ein Kennwortfehler gesendet und die Smartcard kann gesperrt werden.

Authentifizierung mit einer Smartcard durchführen

Die FileArmor Smartcard-Authentifizierung ist nur verfügbar, wenn die entsprechende Richtlinie aktiviert ist. Aktivieren Sie Smartcards in PolicyServer unter folgendem Pfad als Authentifizierungsoption: **FileArmor** > **Anmelden** > **Zulässige Authentifizierungsmethoden**.

Prozedur

1. Öffnen Sie FileArmor und wählen Sie **Smartcard** aus dem Authentifizierungs-Listenfeld aus.
2. Geben Sie den Benutzernamen an.
3. Geben Sie die Smartcard-PIN oder das feste Kennwort an (falls zutreffend).
4. Klicken Sie auf **OK**.

FileArmor ColorCode-Authentifizierung

Die FileArmor ColorCode-Authentifizierung ist nur verfügbar, wenn die entsprechende Richtlinie aktiviert ist. Die Richtlinie ist unter folgendem Pfad verfügbar: **Gruppenname** > **Richtlinien** > **FileArmor** > **Anmelden** > **Zulässige Authentifizierungsmethoden**

Prozedur

1. Wählen Sie **ColorCode** aus dem Authentifizierungs-Listenfeld aus.
2. Geben Sie eine eindeutige ColorCode-Kombination ein.
3. Klicken Sie auf **OK**.

FileArmor PIN-Authentifizierung

Die FileArmor PIN-Authentifizierung ist nur verfügbar, wenn die entsprechende Richtlinie aktiviert ist. Die Richtlinie ist unter folgendem Pfad verfügbar:

Gruppenname > **Richtlinien** > **FileArmor** > **Anmelden** > **Zulässige Authentifizierungsmethoden**.

Prozedur

1. Wählen Sie **PIN** aus dem Authentifizierungs-Listenfeld aus.
2. Geben Sie die PIN-Kombination an.
3. Klicken Sie auf **OK**.

Kennwortänderung in FileArmor

Um das Kennwort zu ändern, muss der Benutzer sich mit dem Benutzerkonto bei FileArmor authentifizieren. Administrator- und Authentifiziererkonten können ihr Kennwort nicht ändern. Das Kennwort kann im Hinblick auf jede beliebige durch die PolicyServer Richtlinien zulässige Methode geändert werden.

Prozedur

1. Klicken Sie mit der rechten Maustaste auf das FileArmor Symbol in der Task-Leiste, und wählen Sie **Kennwort ändern** aus.
2. Geben Sie das Kennwort an und klicken Sie anschließend auf **Weiter**.
3. Wählen Sie eine beliebige, verfügbare Authentifizierungsmethode aus, geben Sie das neue Kennwort an und bestätigen Sie es. Klicken Sie anschließend auf **OK**.

   Das Kennwort wird aktualisiert und eine Bestätigung wird angezeigt.

Erzwungene Kennwortzurücksetzung

FileArmor verhindert den unberechtigten Zugriff auf verschlüsselte Dateien und Ordner, indem geschützte Dateien gesperrt werden, wenn zu viele ungültige Authentifizierungsversuche durchgeführt werden oder wenn für eine bestimmte Dauer keine Kommunikation zwischen Endpunkt und dem PolicyServer erfolgte. Auf Grund

einer Richtlinie sperrt FileArmor den Benutzer für den Zugriff oder aktiviert eine Zeitverzögerung, bevor Authentifizierungsversuche durchgeführt werden können.

Geräte entsperren

Wenn ein Benutzer die Anzahl an Authentifizierungsversuchen überschritten hat und die Remote-Authentifizierung auf Grund von Richtlinien aktiviert ist, sperrt FileArmor Endpoint Encryption Ordner und benachrichtigt den Benutzer, dass Remote-Hilfe erforderlich ist. Die Remote-Hilfe wird verwendet, um FileArmor zu entsperren. Sie erfordert Unterstützung durch einen Unternehmens- oder Gruppenauthentifizierer.

Prozedur

1. Klicken Sie mit der rechten Maustaste auf das FileArmor Symbol in der Task-Leiste, und wählen Sie **Remote-Hilfe** aus.

   Das Fenster **Remote-Hilfe** wird angezeigt.

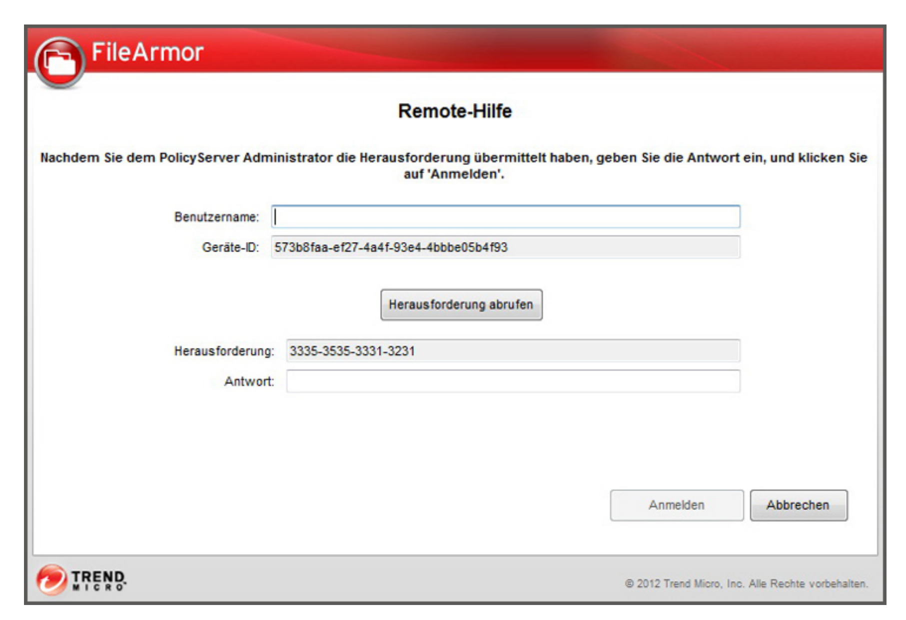


Abbildung 6-1. FileArmor Remote-Hilfe

2. Geben Sie den Benutzernamen an.
3. Klicken Sie auf **Herausforderung abrufen**.
4. Geben Sie die **Antwort** ein, die vom Unternehmens- oder Gruppenauthentifizierer bereitgestellt wurde.
5. Klicken Sie auf **Anmeldung**.

   Der Benutzer wird bei FileArmor authentifiziert und eine Benachrichtigung wird angezeigt.

Zeitverzögerung

Diese gilt für den Fall, dass ein Benutzer die Anzahl der Authentifizierungsversuche überschreitet und auf Grund der Richtlinienkonfiguration eine vorübergehende Zeitverzögerung aktiviert ist, die nicht umgangen werden kann und erst ablaufen muss, bevor eine Authentifizierung zulässig ist.

Nach Ablauf der zulässigen Anzahl an fehlgeschlagenen Authentifizierungsversuchen sperrt FileArmor das Gerät und benachrichtigt den Benutzer diesbezüglich. Während der Zeitverzögerung ist die Möglichkeit zur Anmeldung oder Kennwortzurücksetzung deaktiviert. Die Dauer der Zeitverzögerung wird von der Richtlinie bestimmt. Sobald die Zeitverzögerung abgelaufen ist, darf sich der Benutzer authentifizieren.

FileArmor Task-Leistensymbolmenü

Nach der Installation von FileArmor wird ein Symbol ( ) in der Task-Leiste angezeigt. Das Symbol bietet Zugriff auf zahlreiche FileArmor Funktionen. Klicken Sie mit der rechten Maustaste auf das Symbol, um die Menüelemente anzuzeigen.

TABELLE 6-1. Optionen des FileArmor Task-Leistensymbols

MENÜELEMENT	FUNKTION
Registrieren	Dient der erstmaligen Benutzerregistrierung von FileArmor mit dem PolicyServer. Weitere Informationen finden Sie unter *Erste Authentifizierung bei FileArmor auf Seite 6-2*.
Anmelden/Abmelden	Dient der Authentifizierung mit PolicyServer.
Kennwort ändern	Gestattet den nicht bei der Domäne authentifizierten Benutzern das Ändern ihrer Kennwörter. Weitere Informationen finden Sie unter *Kennwortänderung in FileArmor auf Seite 6-6*.
Remote-Hilfe	Entsperren Sie FileArmor mit Hilfe der Remote-Hilfe, um eine Authentifizierung durchzuführen, wenn das Kennwort vergessen wurde, zu viele Authentifizierungsversuche fehlgeschlagen sind oder das Gerät für eine bestimmte Dauer nicht mit dem PolicyServer kommuniziert hat. Weitere Informationen finden Sie unter *Erzwungene Kennwortzurücksetzung auf Seite 6-6*.
Mit PolicyServer synchronisieren	Laden Sie Richtlinien-Updates manuell vom PolicyServer herunter. Diese Funktion ist hilfreich, um die Konnektivität zum PolicyServer zu testen. Weitere Informationen finden Sie unter *Mit PolicyServer synchronisieren auf Seite 6-10*.
Offline-Dateien mit PolicyServer synchronisieren	Weitere Informationen finden Sie unter *Offline-Dateien mit PolicyServer synchronisieren auf Seite 6-10*.
Benachrichtigung verbergen	Schaltet alle FileArmor Benachrichtigungen aus.
Info über FileArmor	Zeigt Informationen zu FileArmor an, u. a. Version, letzte Synchronisierung und authentifizierte Benutzer. Weitere Informationen finden Sie unter *FileArmor Task-Leistensymbolmenü auf Seite 6-8*.
Schließen	Entfernt das FileArmor Task-Leistensymbol vorübergehend.

Mit PolicyServer synchronisieren

Endpunkt-Clients können neue FileArmor Richtlinien mit Hilfe der Option **Mit PolicyServer synchronisieren** im FileArmor Task-Leistensymbol manuell herunterladen.



Hinweis

- Clients müssen zum Synchronisieren von Richtlinien nicht authentifiziert sein.
- Wenn eine Netzwerkverbindung oder ein PolicyServer nicht verfügbar ist, wird der Fehler **Synchronisierung mit Server konnte nicht durchgeführt werden** angezeigt.

Offline-Dateien mit PolicyServer synchronisieren

Offline-Updates arbeiten mit FileArmor 3.0.13.2447 oder einer höheren Version und neuerdings mit x64-Installationen von FileArmor. Wenn das Update generiert wird, werden alle bestehenden Benutzerkennwörter vom Offline-Update durch das neue feste Kennwort ersetzt.

Beim Update werden Benutzerkennwörter nicht durch synchronisierte Kennwörter ersetzt, um dieselbe Funktionalität der verwalteten Geräte zu gewährleisten.

Zum Hinzufügen eines Benutzers zu einem Offline-Endpunkt-Client ist ein festes Kennwort erforderlich. Der Offline-Prozess generiert die folgenden zwei Dateien:

- Die erste Datei mit der Erweiterung "EXE" wird zum Aktualisieren von bestehenden Full Disk Encryption Geräten verwendet.
- Die zweite Datei mit der Richtlinienaktualisierungserweiterung wird zum Aktualisieren von FileArmor verwendet.



Hinweis

Blackberry Richtlinien werden aus allen neuen Offline-Installationen entfernt, bei denen Blackberry nicht durch eine Lizenzdatei aktiviert wurde. Dadurch wird die Größe der Datei erheblich reduziert.

PolicyServer wechseln

Sie können den PolicyServer, zu dem FileArmor eine Verbindung herstellt, über das Infofenster aktualisieren.

Prozedur

1. Klicken Sie mit der rechten Maustaste auf das FileArmor Symbol in der Task-Leiste, und wählen Sie **Info über FileArmor**.

   Das Fenster **Info** wird angezeigt.

2. Klicken Sie auf **PolicyServer bearbeiten**.

3. Geben Sie den neuen Hostnamen oder die neue IP-Adresse für den PolicyServer ein.

4. Klicken Sie auf **OK**.

   FileArmor wird nun vom neuen PolicyServer verwaltet.

FileArmor Verschlüsselung

Dateien können anhand von FileArmor Richtlinien verschlüsselt werden, die lokal definiert wurden oder auf von PolicyServer definierten Richtlinien basieren. Die verwendete Methode hängt von den Bedürfnissen des Unternehmens- und Endpunktbenutzers für den Dateizugriff und von der gewünschten Sicherheitsstufe ab.

Dateien können automatisch verschlüsselt werden, indem sie in mehreren Speicherorten gespeichert werden:

- Ein Ordner auf dem Gerät
- Ein Ordner auf einem Wechselmedium
- Ein vollständig verschlüsselter Wechseldatenträger

Sie können Dateien auch verschlüsseln, indem Sie mit der rechten Maustaste auf die Datei klicken und eines der folgenden Menüelemente aus dem FileArmor Kontextmenü auswählen:

TABELLE 6-2. FileArmor Kontextmenüelemente

MENÜELEMENT	BESCHREIBUNG
Archivieren	Erstellen Sie eine verschlüsselte Kopie der angegebenen Datei.
Archivieren und brennen	Erstellen Sie eine verschlüsselte Kopie der angegebenen Datei und schreiben Sie diese auf eine CD/DVD.

FileArmor Verschlüsselung mit lokalem Schlüssel

Die Auswahl der Funktion "Lokaler Schlüssel" ermöglicht einem Benutzer, Dateien zu verschlüsseln, die nur dieser Benutzer anzeigen kann.



Hinweis

- Legen Sie die Option **FileArmor** > **Verschlüsselung** > **Zulässige Verschlüsselungsmethode** auf **Eindeutiger Schlüssel des Benutzers** fest.
- Der Zugriff auf lokale Schlüsseldateien kann nur auf einem FileArmor Gerät von dem Benutzer erfolgen, der sie erstellt hat.
- Beim Verschlüsseln einer Datei erstellt FileArmor eine neue Datei. Die Originaldatei verbleibt unverschlüsselt an ihrem ursprünglichen Speicherort.



Warnung!

Je nach Windows Betriebssystem kann ein Benutzer den Inhalt von Ordnern bei einem Benutzerwechsel ohne einen Neustart von Windows anzeigen. Während Dateinamen und Ordnerinhalte angezeigt werden können, ist der Dateiinhalt nicht verfügbar. Dies liegt daran, dass das Windows Betriebssystem die Dateistruktur für die Schnellsuche zwischenspeichert.

Lokale Schlüssel erstellen

Prozedur

1. Klicken Sie mit der rechten Maustaste auf die gewünschte Datei und wählen Sie **FileArmor** > **Archiv** > **Lokaler Schlüssel** aus.

Die Originaldateien bzw. -ordner werden nicht geändert und können aufbewahrt oder gelöscht werden.

FileArmor Verschlüsselung mit gemeinsamem Schlüssel

Dateien können so verschlüsselt werden, dass sie nur von Mitgliedern einer Richtliniengruppe angezeigt werden können, welche die Funktion "Gemeinsamer Schlüssel" verwendet.

- Der Zugriff auf lokale Schlüsseldateien kann nur auf einem FileArmor Gerät von dem Benutzer erfolgen, der sie erstellt hat.
- Legen Sie die beiden Richtlinien folgendermaßen fest: **Zulässige Verschlüsselungsmethode** auf **Eindeutigen Schlüssel gruppieren** und **Verwendeter Verschlüsselungsschlüssel** auf **Gruppenschlüssel**.
- Damit ein FileArmor Benutzer verschlüsselte Dateien in PolicyServer Enterprise anzeigen kann, legen Sie **Verwendeter Verschlüsselungsschlüssel** auf **Unternehmensschlüssel** fest.
- Beim Verschlüsseln einer Datei erstellt FileArmor eine neue Datei. Die Originaldatei verbleibt unverschlüsselt an ihrem ursprünglichen Speicherort.



Warnung!

Je nach Konfiguration der Windows Berechtigungen kann ein Benutzer den verschlüsselten Inhalt von Ordnern bei Benutzerwechseln ohne einen Neustart von Windows anzeigen. Während die Dateinamen und Ordnerinhalte angezeigt werden können, ist der Dateiinhalt nicht verfügbar. Dies liegt daran, dass das Windows Betriebssystem die Dateistruktur für die Schnellsuche zwischenspeichert.

Gemeinsame Schlüssel erstellen

Klicken Sie mit der rechten Maustaste auf die gewünschte Datei und wählen Sie **FileArmor** > **Archiv** > **Gemeinsamer Schlüssel** aus. Die Originaldateien bzw. -ordner werden nicht geändert und können aufbewahrt oder gelöscht werden.

FileArmor Verschlüsselung mit festem Kennwort

FileArmor kann mit einem festen Kennwort verschlüsselte Dateien erstellen. Optional kann die verschlüsselte Datei selbstextrahierend sein. Dies bedeutet, dass der Empfänger zum Entschlüsseln der Datei FileArmor nicht benötigt. Beachten Sie Folgendes:

- Für die Kennwortwiederherstellung bei selbstextrahierenden Dateien steht keine Funktion zur Verfügung. Wenn ein Kennwort vergessen wird, kann die verschlüsselte Datei nicht wiederhergestellt werden.

- Auf Grund einer Einschränkung von Windows dürfen ausführbare (selbstextrahierende) Dateien nicht größer als 2 GB sein.

Einen festen Kennwortschlüssel erstellen

Prozedur

1. Klicken Sie mit der rechten Maustaste auf die gewünschte Datei und wählen Sie **FileArmor** > **Archiv** > **Festes Kennwort** aus.

2. Geben Sie das feste Kennwort an und bestätigen Sie es.



Hinweis

Markieren Sie bei Bedarf die Option **Verschlüsselte Daten als selbstextrahierendes Archiv ausgeben**.

3. Klicken Sie auf **OK**.

   Die Datei wird verschlüsselt.

4. Um die Datei zu entschlüsseln, doppelklicken Sie auf die Datei, geben Sie das Archivkennwort an und klicken Sie anschließend auf **OK**.

5. Doppelklicken Sie bei selbstextrahierenden Archiven auf die Datei, geben Sie das Archivkennwort ein, wählen Sie den Speicherort zum Entpacken aus, entscheiden Sie, ob Sie den Zielordner nach dem Entpacken öffnen oder die vorhandenen Dateien überschreiben möchten und klicken Sie anschließend auf **Fortfahren**.

Die Originaldateien bzw. -ordner werden nicht geändert und können aufbewahrt oder gelöscht werden.

Verschlüsselung digitaler Zertifikate mit FileArmor

FileArmor kann Dateien mit digitalen Zertifikaten (Smartcards) aus dem Windows Zertifikatsspeicher verschlüsseln.

Digitalen Zertifikatsschlüssel erstellen

Prozedur

1. Klicken Sie mit der rechten Maustaste auf die gewünschte Datei und wählen Sie **FileArmor** > **Archiv** > **Zertifikat** aus.
2. Wählen Sie einen **Zertifikatsspeicher** aus und klicken Sie anschließend auf **Zertifikate sammeln**.
3. Wählen Sie mindestens ein Zertifikat aus und klicken Sie anschließend auf **OK**.



Hinweis

Zertifikate werden aus dem Windows Zertifikatsspeicher gesammelt.

4. Wählen Sie ein optisches Laufwerk aus und legen Sie eine leere CD/DVD ein.
5. Klicken Sie auf **OK**.

Die Originaldateien bzw. -ordner werden nicht geändert und können aufbewahrt oder gelöscht werden.

FileArmor – Archivieren und brennen

Mit der FileArmor Funktion **Archivieren und brennen**können verschlüsselte Dateien auf CD/DVD geschrieben werden. Die Dateien sind selbstextrahierend und können mit einem festen Kennwort oder digitalen Zertifikat verschlüsselt werden.

Archiv mit einem festen Kennwort brennen

Prozedur

1. Klicken Sie mit der rechten Maustaste auf die Datei und wählen Sie im FileArmor Kontextmenü **FileArmor** > **Archivieren und brennen** > **Festes Kennwort**.
2. Geben Sie ein Kennwort an und bestätigen Sie es.
3. Wählen Sie ein Laufwerk aus, in dem eine beschreibbare Disc eingelegt ist.
4. Klicken Sie auf **OK**.

   Die selbstextrahierende Datei wird auf die CD/DVD gebrannt.

Archiv mit einem Zertifikat brennen

Prozedur

1. Klicken Sie mit der rechten Maustaste auf die Datei und wählen Sie im FileArmor Kontextmenü **FileArmor** > **Archivieren und brennen** > **Zertifikat**.
2. Wählen Sie einen **Zertifikatspeicher** aus und klicken Sie auf **Zertifikate sammeln**.
3. Wählen Sie ein oder mehrere Zertifikate aus und klicken Sie auf **OK**.
4. Wählen Sie ein optisches Laufwerk aus, in dem eine leere CD/DVD eingelegt ist.
5. Klicken Sie auf **OK**.

Die selbstextrahierende Datei wird auf die CD/DVD gebrannt.

FileArmor Sicheres Löschen

FileArmor bietet eine sichere Löschfunktion, mit der die ausgewählten Dateien und der Dateiverlauf von Ihrem Gerät rückstandsfrei entfernt und per Wipe und Erase gelöscht werden.

Prozedur

1. Klicken Sie mit der rechten Maustaste auf die Datei und navigieren Sie zu **FileArmor** > **Sicheres Löschen**.
2. Klicken Sie auf **Ja**, um die Datei dauerhaft zu löschen.



Kapitel 7

Mit KeyArmor arbeiten

KeyArmor USB-Laufwerke schützen Daten mit ständig verfügbarer Hardware-Verschlüsselung und integriertem Antivirus-/Anti-Malware-Schutz, um strenge gesetzliche Vorschriften und Richtlinien zu erfüllen. Mit KeyArmor haben Administratoren vollständige Transparenz und Kontrolle darüber, wer USB-Geräte zu welchem Zeitpunkt, an welchem Ort im Unternehmen und auf welche Weise einsetzt.

Dieses Kapitel umfasst folgende Themen:

- *KeyArmor Funktionen auf Seite 7-4*
- *KeyArmor Authentifizierung auf Seite 7-2*
- *KeyArmor verwenden auf Seite 7-6*

KeyArmor Authentifizierung

Die KeyArmor Authentifizierung hat die Funktion, Benutzern eine Auswahl an Identifizierungsmethoden bereitzustellen. Diese Auswahl bietet Flexibilität und kann genutzt werden, um den Sicherheitsanforderungen des Unternehmens zu entsprechen. Eine erfolgreiche Authentifizierung ermöglicht einem Benutzer den Zugriff auf das Gerät.

Weitere Informationen zur Endpoint Encryption Authentifizierung finden Sie unter *Kontenrollen und Authentifizierung auf Seite 1-13*.

Erste Authentifizierung bei KeyArmor

Prozedur

1. Schließen Sie das KeyArmor Flash-Gerät an einen USB-Port an, um die Software zu starten.
    - Wenn KeyArmor automatisch startet, wird die Statusleiste angezeigt und das KeyArmor Symbol wird der Task-Leiste hinzugefügt.
    - Wenn KeyArmor nicht automatisch startet, navigieren Sie zu "Mein Gerät" und öffnen Sie das KeyArmor Laufwerk.
2. Geben Sie den Benutzernamen und das Kennwort ein.
3. Geben Sie den PolicyServer im Feld **Host-Name** oder **IP-Adresse** an.
4. Geben Sie den Unternehmensnamen im Feld **Name des Unternehmens** an.
5. Klicken Sie auf **Anmelden**.

Authentifizierungsmethode ändern



Hinweis

- Es ist nur eine Authentifizierungsmethode für einen bestimmten Benutzer zu einem beliebigen Zeitpunkt gültig.
- Ein Benutzer kann die Authentifizierungsmethode nur nach einer erfolgreichen Anmeldung am KeyArmor Gerät ändern.

Prozedur

1. Klicken Sie mit der rechten Maustaste auf das KeyArmor Symbol in der Task-Leiste, und wählen Sie **Kennwort ändern** aus.

   Das Fenster **Wird geladen** wird gefolgt vom Fenster **Kennwort ändern** für die aktuelle Authentifizierungsmethode des Benutzers angezeigt.

2. Klicken Sie auf **Authentifizierung**.
3. Wählen Sie eine neue Authentifizierungsmethode aus.
4. Geben Sie das aktuelle Kennwort an.
5. Klicken Sie auf **Ändern**, um Fenster mit der neuen Authentifizierungsmethode anzuzeigen.

   Das Fenster **Ändern der Authentifizierungsmethode abgeschlossen** wird angezeigt.

Festes Kennwort

Feste Kennwörter bilden die häufigste Methode zum Identifizieren von Benutzern. Das Kennwort wird vom Benutzer gewählt. Navigieren Sie zum Konfigurieren von Richtlinienbeschränkungen für Kennwörter zu **KeyArmor** > **Anmelden** auf Gruppen- oder Unternehmensebene.



Hinweis

Als Erstauthentifizierung bei KeyArmor wird immer ein festes Kennwort verwendet.

Prozedur

1. Geben Sie das neue feste Kennwort an und bestätigen Sie es.
2. Wählen Sie eine der folgenden Optionen:
   - Klicken Sie zum Durchführen der Kennwortänderung auf **Ändern**.
   - Wenn Sie die Feldinhalte entfernen möchten, klicken Sie auf **Löschen**.

   Der Benutzer wird bei KeyArmor authentifiziert und kann nun Daten im Ordner **SICHERE DATEN** speichern. Das KeyArmor Symbol wird in der Task-Leiste angezeigt.

KeyArmor Funktionen

In diesem Abschnitt werden die wichtigsten Funktionen von KeyArmor erläutert.

Gerätekomponenten

KeyArmor stellt zwei Laufwerke bereit, wenn Sie das Gerät an einen USB-Port anschließen.

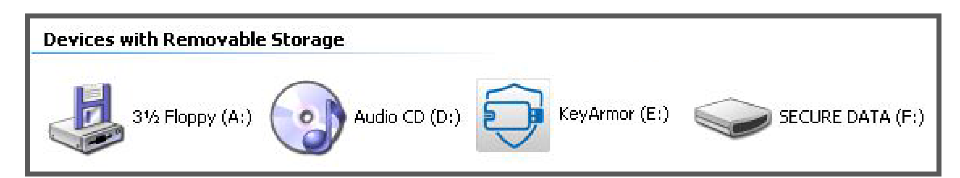


ABBILDUNG 7-1. KeyArmor Geräte

- **KeyArmor (E:)** enthält die Programmdateien von KeyArmor.

- **SECURE DATA (F:)** ist das Benutzerspeichergerät von KeyArmor. KeyArmor verschlüsselt alle auf diesem Laufwerk gespeicherten Dateien.

Dateien mit KeyArmor schützen

Um Dateien mit KeyArmor zu schützen, kopieren oder ziehen Sie die entsprechenden Ordner, Dateien oder Dokumente auf das KeyArmor Laufwerk "SICHERE DATEN".

Auf KeyArmor gespeicherte Dateien werden automatisch verschlüsselt. Es kann nur mit gültigen Endpoint Encryption Anmeldedaten auf sie zugegriffen werden. Die Dateien bleiben verschlüsselt, solange sie auf KeyArmor gespeichert sind.



Hinweis

Um sicherzustellen, dass die Antivirusdefinitionen aktuell sind, kopieren Sie Dateien erst auf das KeyArmor Gerät, nachdem die ersten Antivirus-Updates durchgeführt wurden.

Keine Informationen hinterlassen

KeyArmor kann auf verschiedene Arten verhindern, dass Informationen auf dem lokalen Gerät zurückbleiben:

- Beim Durchsuchen von Dateien auf dem KeyArmor Gerät werden keine Daten auf den Host kopiert.
- Beim Öffnen und Bearbeiten von Dokumenten mit Hilfe von Anwendungen auf dem Host können temporäre Dateidaten oder Daten zur Dateiwiederherstellung auf dem Host gespeichert werden.
- Die meisten Softwareanwendungen verfügen über die Konfigurationsmöglichkeit, ihre temporären Dateidaten oder Daten zur Dateiwiederherstellung auf dem KeyArmor Gerät zu speichern.

KeyArmor Antivirus-Updates und -aktivitäten

Nach der Authentifizierung wird versucht, ein Update der KeyArmor Antivirusdefinitionen durchzuführen. KeyArmor gibt Warnungen über Antivirus-Update-Aktivitäten aus.



Warnung!

Melden Sie ein KeyArmor Gerät nicht vom Endpunkt-Client ab bzw. entfernen Sie es nicht, während das Antivirus-Update durchgeführt wird.

Das Kopieren oder Öffnen von Dateien aus KeyArmor ist eine vom Endbenutzer eingeleitete Aktivität. Dateien werden beim Speichern oder Kopieren auf KeyArmor durchsucht. Im Fall, dass ein Virus gefunden wird, steuert der Systemadministrator das daraus resultierende weitere Vorgehen, wie z. B. Reparatur- und Löschversuche oder eine Wipe-Löschung des gesamten KeyArmor Geräts. Benutzer können möglicherweise nach der Authentifizierung eine vollständige Suche ihres KeyArmor Geräts einleiten.

KeyArmor Benachrichtigung zur Festplattenüberprüfung

Das unsachgemäße, nicht sichere Entfernen eines KeyArmor Geräts kann zu Schäden am Dateisystem führen. Melden Sie sich von KeyArmor immer ab, bevor Sie das Gerät physisch entfernen. Wenn das Gerät nicht ordnungsgemäß heruntergefahren oder nicht sicher entfernt wurde oder wenn andere unvorhergesehene Umstände eingetreten sind, werden Sie möglicherweise dazu aufgefordert, die Festplatte beim nächsten Einfügen des Schlüssels zu überprüfen. Sie können diese Aufforderung getrost ignorieren und fortfahren. KeyArmor überprüft die Festplatte für Sie und korrigiert mögliche Fehler.

KeyArmor verwenden

In diesem Abschnitt wird die Verwendung von KeyArmor beschrieben.

Warnung zu unverschlüsselten Geräten

- KeyArmor Benutzer sollten die Unternehmensrichtlinie befolgen, die sich auf die Übertragung von Daten auf nicht speziell einem Benutzer zugewiesene Arbeitsgeräte bezieht.
- KeyArmor verschlüsselt alle gespeicherten Dateien.

- Die KeyArmor Software wird über das Gerät ausgeführt. Zu keiner Zeit kopiert die KeyArmor Software Daten auf das Host-Gerät.
- Beim Durchsuchen von Dateien auf dem Gerät werden ebenfalls keine Daten auf das Host-Gerät kopiert.
- Das Kopieren von Dateien auf ein Host-Gerät ist eine vom Benutzer initiierte Aktion, die ausschließlich nach einer ordnungsgemäßen Anmeldung am Gerät durchgeführt werden kann.
- Bestimmte auf dem Host ausgeführte Softwareanwendungen speichern temporäre oder Daten aus einer Wiederherstellungsdatei auf dem Host-Gerät.
- Die meisten Softwareanwendungen können so konfiguriert werden, dass temporäre oder Daten aus einer Wiederherstellungsdatei auf dem KeyArmor Gerät gespeichert werden. Diese Aktion wird empfohlen, wenn das Gerät außerhalb der Grenzen des vertrauenswürdigen/sicheren Netzwerks verwendet werden soll.

KeyArmor Taskleiste

Mehrere Optionen sind verfügbar, wenn KeyArmor über die Taskleiste geöffnet wird:

TABELLE 7-1. KeyArmor Taskleiste

MENÜELEMENT	FUNKTION
Vollständige Suche starten	Durchsucht das KeyArmor Gerät auf Bedrohungen.
Richtlinien-Updates herunterladen	Lädt die aktuellen Richtlinien-Updates herunter. Wenn der Administrator beispielsweise eine neue Authentifizierungsmethode hinzufügt und die vorhandenen Authentifizierungsmethoden entfernt, wird der Benutzer unter Umständen angewiesen, die Richtlinien-Updates herunterzuladen und sofort die neue Authentifizierungsmethode zu verwenden.
Kennwort ändern	Gestattet den nicht bei der Domäne authentifizierten Benutzern das Ändern ihrer Kennwörter.
Sichere Daten öffnen	Öffnet das Laufwerk "Sichere Daten".

Menüelement	Funktion
Info über KeyArmor	Zeigt KeyArmor Informationen an, einschließlich der Version, der letzten Synchronisierung und des authentifizierten Benutzers.
Abmelden	Meldet KeyArmor ab.

KeyArmor Menü

Verschiedene Optionen stehen im KeyArmor Menü zur Verfügung:

Tabelle 7-2. KeyArmor Menüelemente

Menüelement	Beschreibung
Authentifizierung	Weitere Informationen finden Sie unter *KeyArmor Authentifizierung auf Seite 7-2*.
Richtlinien-Updates herunterladen	Laden Sie die aktuellen Richtlinien-Updates herunter. Wenn der Administrator beispielsweise eine neue Authentifizierungsmethode hinzufügt und die vorhandenen Authentifizierungsmethoden entfernt, wird der Benutzer unter Umständen angewiesen, die Richtlinien-Updates herunterzuladen und sofort die neue Authentifizierungsmethode zu verwenden.
Hilfe	Weitere Informationen finden Sie unter *KeyArmor Hilfemenü auf Seite 7-8*.

KeyArmor Hilfemenü

Das Menü "KeyArmor Hilfe" verfügt über mehrere Optionen zur Benutzerunterstützung.

Falls gefunden

Wenn ein KeyArmor Gerät verloren geht und von einer anderen Person als dem Gerätebesitzer gefunden wird, bietet die Option **Falls gefunden** Kontaktinformationen, mit deren Hilfe der Finder das Gerät an seinen rechtmäßigen Besitzer zurückgeben

kann. Diese Option steht jedem Benutzer zur Verfügung, ohne dass entsprechende Anmeldedaten eingegeben werden müssen.

Die Meldung **Falls gefunden** wird als Richtlinie im PolicyServer erstellt.

Prozedur

1. Navigieren Sie zum Erstellen einer **Falls gefunden**-Meldung zu **KeyArmor** > **Hinweismeldungen**.

2. Klicken Sie mit der rechten Maustaste auf **Falls gefunden** und wählen Sie dann **Eigenschaften** aus.

Das Fenster **Richtlinienwert bearbeiten** wird geöffnet.

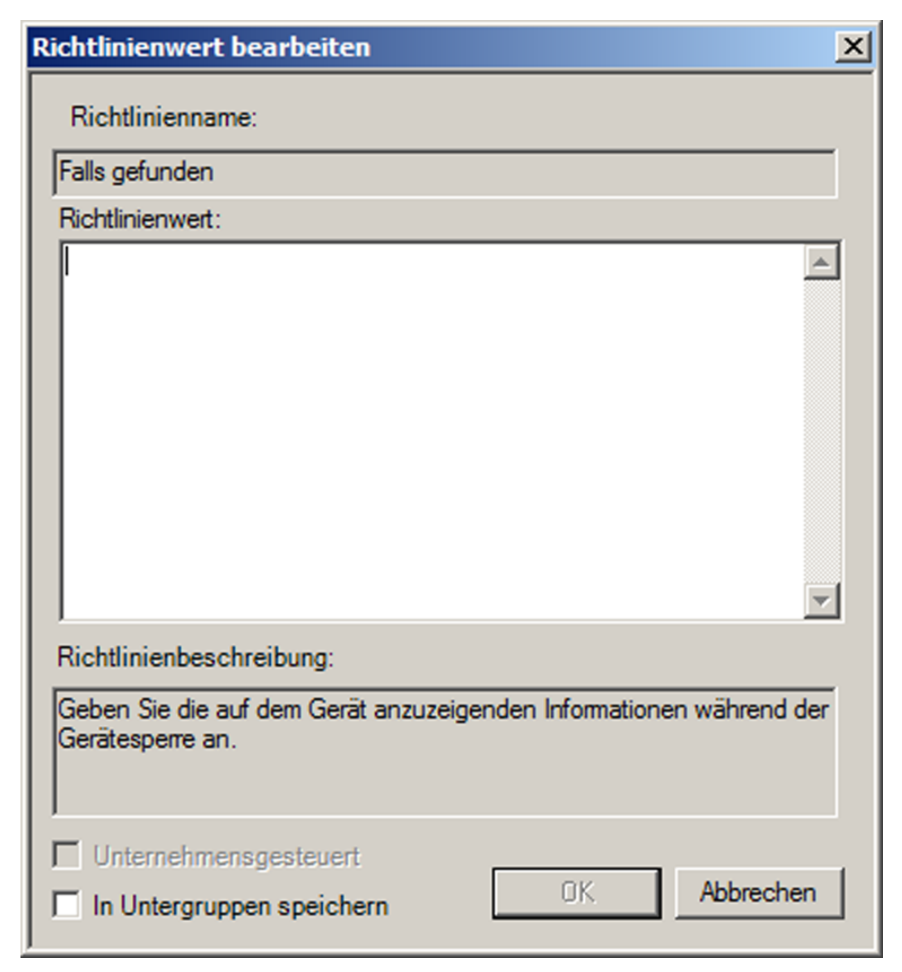


ABBILDUNG 7-2. Falls gefunden-Richtlinie bearbeiten

3. Geben Sie die Meldung **Falls gefunden** im Feld **Richtlinienwert** ein.

4. Klicken Sie auf **Übernehmen**.

F/A-Kennwortzurücksetzung

Die Selbsthilfe ermöglicht Benutzern, auf eine oder mehrere vordefinierte Fragen zu antworten. Die Fragen der Selbsthilfe werden als Richtlinien im PolicyServer erstellt.

So definieren Sie die Fragen:

Prozedur

1. Navigieren Sie zu **Allgemein** > **Authentifizierung** > **Lokale Anmeldung** > **Selbsthilfe**.
2. Klicken Sie mit der rechten Maustaste auf **Anzahl der Fragen** und wählen Sie **Eigenschaften** aus.
3. Geben Sie im Feld **Richtlinienwert** die Anzahl an Fragen ein, die richtig beantwortet werden müssen.
4. Klicken Sie auf **Übernehmen**.
5. Klicken Sie mit der rechten Maustaste auf **Persönliche Herausforderung** und klicken Sie dann auf **Hinzufügen**.
6. Öffnen Sie die angezeigte Richtlinie **Persönliche Herausforderung**, geben Sie eine Frage im Feld **Richtlinienwert** ein und klicken Sie dann auf **Übernehmen**.



Hinweis

Alle der Gruppe, in der die Fragen erstellt werden, zugewiesenen Benutzer werden aufgefordert, gemäß der neuen Richtlinieneinstellung eine Antwort auf jede Frage bereitzustellen, wenn sich der Benutzer erstmalig anmeldet.

Remote-Kennwortzurücksetzung

Bei der Remote-Hilfe handelt es sich um einen Prozess, mit dem der Benutzer ein vergessenes Kennwort remote zurücksetzen lassen kann. Bei Verwendung der Remote-Hilfe muss der Benutzer erstens in der Lage sein, das Helpdesk zu kontaktieren, und zweitens über Zugriff auf die Option "Remote-Kennwortzurücksetzung" im Menü "KeyArmor Hilfe" verfügen.

Prozedur

1. Der Benutzer wählt **Remote-Kennwortzurücksetzung** im Menü **Hilfe** aus.
2. Der Benutzer wendet sich an den PolicyServer Administrator.
3. Der Benutzer übermittelt dem Support-Mitarbeiter die **Geräte-ID**.
4. Der Support-Mitarbeiter sucht in der PolicyServer MMC nach der **Geräte-ID** und klickt mit der rechten Maustaste auf das Gerät, um die Menüoptionen anzuzeigen. Anschließend klickt der Mitarbeiter auf "Soft-Token".
5. Der Benutzer übermittelt die **Herausforderung** an den Administrator.
6. Der Administrator gibt die Herausforderung im Feld **Herausforderung** ein, klickt auf **Antwort erhalten** und übermittelt die **Antwort** an den Benutzer.
7. Der Benutzer gibt die Antwort im Feld **Antwort** ein und klickt dann auf **Anmeldung**.

   Dem Benutzer wird ein Bildschirm zum Ändern des Kennworts angezeigt, der auf der aktuellen Authentifizierungsmethode basiert.
8. Der Benutzer muss das neue Kennwort angeben und bestätigen.

Support-Informationen

Das Fenster "Support-Informationen" enthält in der Regel Kontaktinformationen für das Unternehmens-Helpdesk.

Info über KeyArmor

Der Bildschirm "Info über KeyArmor" wird automatisch ausgefüllt und enthält folgende Informationen:

- Software version
- Benutzername
- PolicyServer Adresse
- Unternehmen

- Gerätename
- Letzte Richtliniensynchronisierung
- FIPS-Version

Dateien mit KeyArmor schützen

Mit KeyArmor können Sie Ihre Dateien problemlos schützen. Sie müssen die ausgewählten Dateien/Dokumente lediglich auf das KeyArmor Laufwerk kopieren oder ziehen. Alle auf dem KeyArmor Gerät gespeicherten Dateien und Ordner werden automatisch verschlüsselt. Zum Zugriff auf die Dateien ist die Anmeldung am Gerät mit einem gültigen Benutzernamen und einem Kennwort erforderlich.

- Alle auf KeyArmor gespeicherten Dateien und Ordner werden automatisch verschlüsselt.
- Die Dateien bleiben verschlüsselt, solange sie auf KeyArmor gespeichert sind.

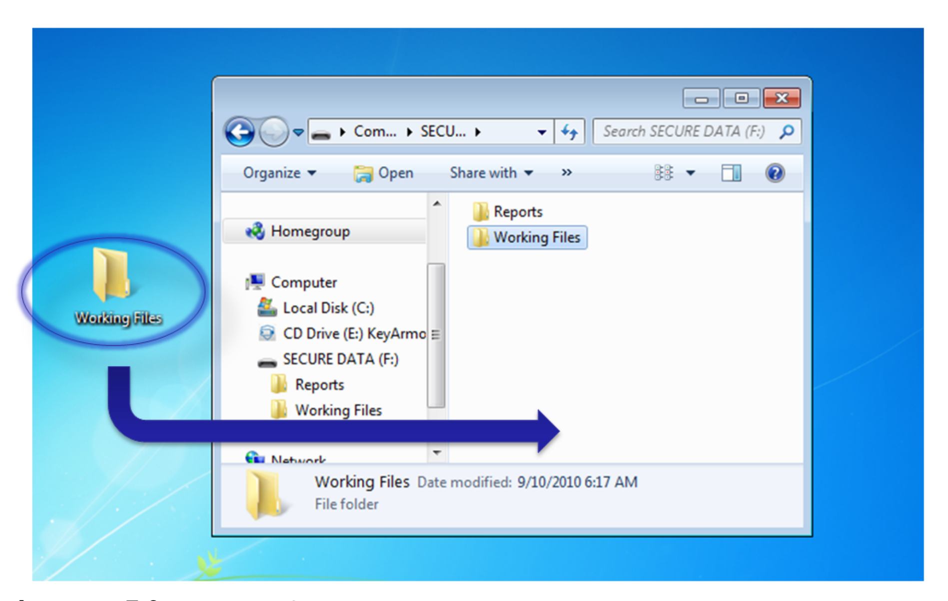


ABBILDUNG 7-3. Dateien auf KeyArmor kopieren

KeyArmor Aktivitätsprotokollierung

Alle KeyArmor Aktivitäten werden protokolliert und transparent über das Netzwerk auf den PolicyServer hochgeladen. Die PolicyServer MMC bietet Zugriff auf Standardberichte und ausführliche Aktivitätsprotokolle. Administratoren können einen Drilldown zu einer bestimmten Geräte-, Datei- und Endbenutzeraktivität durchführen. Weitere Informationen zu KeyArmor Richtlinien finden Sie unter *KeyArmor Richtlinien auf Seite 3-37*.

KeyArmor sicher entfernen

Entfernen Sie ein KeyArmor Gerät wie jedes andere USB-Speichergerät sicher, bevor Sie es vom USB-Port trennen.



Warnung!

Die Daten und/oder das Gerät können beschädigt werden, wenn KeyArmor unsachgemäß vom Computer entfernt wird.

Wählen Sie eine der folgenden Option aus, um ein authentifiziertes KeyArmor Gerät sicher zu entfernen.

- Bei Auswahl von **Abmelden** auf der KeyArmor Benutzeroberfläche (Anwendungsfenster oder Rechtsklick auf die Taskleiste) wird das Gerät sicher ausgeworfen.
- Klicken Sie mit der rechten Maustaste auf das KeyArmor Symbol in der Task-Leiste, und wählen Sie **Abmelden** aus.

Nach der Abmeldung steht KeyArmor in der Windows Safely Remove Hardware-Anwendung nicht mehr zur Verfügung. Das Gerät kann nun sicher aus dem USB-Port des Computers entfernt werden.

Um ein nicht authentifiziertes KeyArmor Gerät sicher auszuwerfen, schließen Sie vor der Übermittlung der Anmeldedaten das Dialogfeld für die Authentifizierung.

Vollständige Suche von KeyArmor

Nach der Authentifizierung versucht KeyArmor, ein Update der Antivirusdefinitionen durchzuführen. KeyArmor gibt Warnungen über Antivirus-Update-Aktivitäten aus. Melden Sie ein KeyArmor Gerät nicht vom Host-PC ab bzw. entfernen Sie es nicht, während das Antivirus-Update durchgeführt wird. Dateien werden beim Speichern oder Kopieren auf KeyArmor nach Viren durchsucht.

Im Fall, dass ein Virus gefunden wird, steuern die PolicyServer Richtlinien das daraus resultierende weitere Vorgehen, wie z. B. Reparatur- und Löschversuche oder eine Wipe-Löschung des gesamten KeyArmor Geräts. Außerdem hat der Client die Möglichkeit, eine vollständige Suche des KeyArmor Geräts einzuleiten.

TABELLE 7-3. FileArmor Antivirusaktivitäten

AKTIVITÄT	BESCHREIBUNG
Antivirus-Updates	Nachdem die Antivirusdefinitionen geladen wurden, führt KeyArmor die Updates der Definitionen gemäß der Richtlinie durch.
Dateien durchsuchen	Dateien werden beim Kopieren auf KeyArmor nach Viren durchsucht. Dateien, die Viren enthalten, werden nicht auf das geschützte Gerät kopiert.
Gerät vollständig durchsuchen	Sie können über das KeyArmor Symbol in der Task-Leiste eine vollständige Suche einleiten. Navigieren Sie hierfür zu **KeyArmor** > **Vollständige Suche starten**.

Den Standard-Update-Speicherort für den Virenschutz ändern

Neben der Standard-Update-Adresse können Sie einen anderen HTTP- oder FTP-Speicherort einrichten, in den KeyArmor Updates für seine Virenschutzkomponenten herunterladen kann.



Hinweis

- Standardmäßig ist die KeyArmor Richtlinie so konfiguriert, dass Updates automatisch aus folgendem Speicherort heruntergeladen werden: FTP://download.trendmicro.com/products/pattern/
- Administratoren können diese Richtlinie derart ändern, dass KeyArmor Virenschutz-Updates aus anderen Remote-Host-Speicherorten oder einer lokalen Quelle mit Hilfe der im Folgenden erläuterten HTTP- oder FTP-Konventionen abrufen kann.

Prozedur

1. So richten Sie eine HTTP-Adresse ein:
   a. Kopieren Sie auf dem FTP-Server von Trend Micro alle ZIP-Dateien, die mit den Buchstaben "LPT" beginnen, sowie die Datei "`opr.ini`" und legen Sie sie am ausgewählten Speicherort des HTTP-Hosts ab.
   b. Weisen Sie die KeyArmor Geräte an, die Virenschutzdefinitionen aus dem HTTP-Webordner herunterzuladen, indem Sie die vollständige URL für die Updates im Richtlinienwert **KeyArmor** > **Virenschutz** > **Update-Adresse** festlegen.

      Hosten Sie diese Dateien beispielsweise auf dem PolicyServer Computer, indem Sie sie im Hauptwebverzeichnis ablegen: `c:\inetpub\wwwroot\mawebservice2\`
2. So richten Sie eine FTP-Adresse ein:
   a. Installieren Sie den FTP-Dienst von Microsoft IIS oder andere FTP-Server-Software und konfigurieren Sie einen FTP-Ordner zur Verwendung für Netzwerk-Clients.
   b. Kopieren Sie alle ZIP-Dateien, die mit "lpt" beginnen, sowie die Datei `opr.ini` aus dem Trend Micro Download-Speicherort in das Verzeichnis des konfigurierten FTP-Servers (beispielsweise `c:\inetpub\ftpsvc\`)
   c. Weisen Sie die KeyArmor Geräte an, die Virenschutzdefinitionen aus dem HTTP-Ordner herunterzuladen, indem Sie die vollständige URL im Richtlinienwert **KeyArmor** > **Virenschutz** > **Update-Adresse** festlegen.

Nächste Maßnahme

Trend Micro empfiehlt, diese Konfigurationsänderung zu testen, indem Sie Richtlinien auf einem registrierten KeyArmor Gerät synchronisieren und Folgendes überprüfen:

1. Virenschutz-Updates wurden erfolgreich durchgeführt.
2. Virenschutzdefinitionen wurden auf dem Schlüssel aktualisiert.
3. In den PolicyServer Protokolleinträgen wird die in der neuen Richtlinie definierte URL angezeigt.

Ein KeyArmor Gerät einem anderen Benutzer neu zuweisen

KeyArmor kann so konfiguriert werden, dass alle Benutzer in einer Gruppe oder ein einzelner Benutzer Zugriff auf ein Gerät erhält. Um diese Richtlinie zu ändern, legen Sie **KeyArmor** > **Anmeldung** > **Nur einen Benutzer pro Gerät zulassen** fest. Ist "Nur einen Benutzer pro Gerät zulassen" auf **Ja** gesetzt, kann nur ein Benutzer zu einem bestimmten Zeitpunkt auf das Gerät zugreifen.



Hinweis

Diese Richtlinie wirkt sich nicht auf Administrator- bzw. Authentifiziererrollen aus.

Prozedur

1. Melden Sie sich an der PolicyServer MMC an und navigieren Sie zu der Gruppe, der das Gerät zugewiesen wurde.
2. Entfernen Sie das Gerät, indem Sie mit der rechten Maustaste auf die Geräte-ID klicken und **Gerät entfernen** auswählen.



Hinweis

- Entfernen Sie die KeyArmor Geräte-ID nicht aus Ihrem Unternehmen. Ansonsten kann auf das Gerät nicht mehr zugegriffen werden.
- Es wurden Sicherheitsvorkehrungen getroffen, um die erneute Bindung von KeyArmor an ein weiteres Unternehmen zu verhindern, sobald eine Verbindung zu Ihrem Unternehmen erstellt wurde.
- Dieselbe Logik verhindert, dass KeyArmor dem Unternehmen erneut hinzugefügt wird, sollten Sie die Geräte-ID versehentlich vom PolicyServer löschen.

3. Schließen Sie das KeyArmor Gerät an einen PC an und synchronisieren Sie die Richtlinien.
4. Kehren Sie zur MMC zurück und fügen Sie das Gerät zur benötigten Gruppe hinzu.
5. Stellen Sie sicher, dass der neue Benutzer ein Mitglied der benötigten Gruppe ist.
6. Weisen Sie dem Benutzer ein festes Kennwort zu.
7. Verteilen Sie das Gerät an den neuen Benutzer und weisen Sie ihm einen Benutzernamen und ein Kennwort zu.
8. Das Gerät wird nun an den neuen Benutzer gebunden.



Warnung!

Alle auf dem Gerät verbliebenen Daten des vorherigen Benutzers stehen dem neuen Benutzer zur Verfügung. Administratoren sollten die internen Richtlinien für die erneute Formatierung oder erneute Bereitstellung eines Geräts befolgen, bevor sie KeyArmor einem neuen Benutzer zuweisen.

Ein gelöschtes KeyArmor Gerät wieder zum Unternehmen hinzufügen

Wenn ein Gerät versehentlich gelöscht wird, kann es zum Unternehmen mit einer der beiden folgenden Methoden wieder hinzugefügt werden:

Prozedur

1. **Automatisch**: Wenn ein Benutzer an einem mit PolicyServer verbundenen Gerät angemeldet wird, wird das Gerät während der nächsten Gerätesynchronisierung automatisch wieder zum Unternehmen hinzugefügt.

   a. Ein Unternehmensadministrator muss das Gerät dennoch in die richtige Gruppe verschieben, um einen kontinuierlichen Benutzerzugriff auf das Gerät sicherzustellen.



Hinweis

- Als Best Practice wird empfohlen, das Gerät vor dem Löschen zu sperren oder zu entfernen.
- Ein aus dem Unternehmen gelöschtes Gerät wird gesperrt, wenn Richtlinien eine Kommunikation mit PolicyServer erfordern.

2. **Manuell**: Als Administrator können Sie folgende Schritte durchführen:



Hinweis

Dies erfordert Konnektivität mit dem neuen Enterprise PolicyServer.

   a. Melden Sie sich am Gerät mit einer gültigen Unternehmensadministrator-ID und dem gültigen Kennwort an.

   b. Klicken Sie mit der rechten Maustaste auf das KeyArmor Symbol in der Task-Leiste, und wählen Sie **Info über KeyArmor** aus.

   c. Klicken Sie auf **Bearbeiten** neben dem Feld für den Namen des Unternehmens.

   d. Vergewissern Sie sich, dass der Name des Unternehmens richtig ist.

   e. Wählen Sie **OK**.

   f. Wählen Sie **Schließen**.

g. Nun muss der Unternehmensadministrator das Gerät einer Gruppe wieder hinzufügen, um es Benutzern zur Verfügung zu stellen.



Kapitel 8

Arbeiten mit Protokollen und Berichten

Endpoint Encryption erstellt umfassende Protokolle und generiert Berichte über Ereignisse und Aktualisierungen. Verwenden Sie diese Protokolle und Berichte, um die Richtlinien Ihres Unternehmens zu bewerten und um die erfolgreiche Aktualisierung von Komponenten sicherzustellen.

Dieses Kapitel umfasst folgende Themen:

- *Protokollereignisse auf Seite 8-2*
- *Berichte auf Seite 8-6*

Protokollereignisse

PolicyServer zeichnet Protokollereignisse unter Verwendung vordefinierter Kriterien auf, die in das System integriert sind, wie z. B. Zugriffsversuche, Systemfehler, Änderungen an Benutzern oder Gruppen, Richtlinienänderungen sowie Probleme bei der Einhaltung von Richtlinien. Dieses leistungsfähige Tool kann verwendet werden, um alle Aspekte der Server- und Client-Sicherheit aufzuzeichnen. Die Verwaltung von Protokollereignissen ermöglicht einem Gruppen- oder Unternehmensadministrator die Auswahl bestimmter Suchkriterien, die auf dem Bildschirm angezeigt werden können.

Protokollereignisse verwalten

Nur Nachrichten der letzten sieben Tage werden automatisch angezeigt. Verwenden Sie die Filterfunktion, um ältere Nachrichten anzuzeigen. Es ist sinnvoll, die Protokolle mit Hilfe der **Nachrichten-ID** zu durchsuchen. Wenn Sie beispielsweise nach der Nachrichten-ID 400008 suchen, werden alle "Geräteverschlüsselung abgebrochen"-Nachrichten angezeigt. Weitere Einzelheiten finden Sie unter *PolicyServer Nachrichten-IDs auf Seite A-1*.

Prozedur

1. Es gibt zwei Ebenen für Protokollereignisse:

    - Für Protokolle auf Unternehmensebene erweitern Sie **Unternehmen - Protokollereignisse**.

    - Für Protokolle auf Gruppenebene navigieren Sie zu **Gruppenname** > **Protokollereignisse.**

    Das Fenster "Protokoll" wird angezeigt. Alle Ereignisse der letzten sieben Tage werden automatisch angezeigt.

2. Doppelklicken Sie auf ein beliebiges Protokoll, um Details anzuzeigen.

3. Klicken Sie auf **Filter**, um nach der Protokolldatei zu suchen:

    a. Geben Sie die Suchkriterien an.

    b. Wählen Sie den Datumsbereich aus.

c. Klicken Sie auf **Suchen**.

4. Klicken Sie auf **Aktualisieren**, um die Protokolldaten zu aktualisieren.

5. Klicken Sie auf **Vorherige** oder **Nächste**, um durch die Protokolldaten zu navigieren.

Warnungen

Administratoren können Alarmkriterien anpassen, indem sie vordefinierte Sicherheitsebenen für die Kategorisierung von Alarmen verwenden. Senden Sie Protokollereignisse an einen einzelnen oder mehrere E-Mail-Empfänger, indem Sie Alarme im Unternehmen oder in der Gruppe einrichten.



Hinweis

Einzelheiten zu Nachrichten-IDs finden Sie unter *PolicyServer Nachrichten-IDs auf Seite A-1*.

PolicyServer Warnungen einrichten

Prozedur

1. Wählen Sie in der PolicyServer MMC im linken Navigationsbildschirm die Option **Unternehmens- oder Gruppenprotokollereignisse** aus.

2. Klicken Sie auf **Warnungen**.

3. Klicken Sie mit der rechten Maustaste und wählen Sie **Hinzufügen** aus.

   Das Fenster "Warnung bearbeiten" wird geöffnet.

4. Nehmen Sie unter **Warnungsname** eine Eingabe vor.

5. Wählen Sie den Schweregrad von Protokollen aus, die Warnungen auslösen.

6. Wählen Sie die Nachrichten-IDs aus, die Warnungen auslösen.

7. Geben Sie pro Zeile eine E-Mail-Adresse für den Empfang von Warnungen an.

8. Geben Sie an, ob Warnungen basierend auf der Anzahl von Ereignissen während eines festgelegten Zeitraums gesendet werden sollen.

9. Klicken Sie auf **Fertig**.

PolicyServer zur Weiterleitung von SMS und E-Mail-Versand aktivieren

Diese Funktion kann nur auf PolicyServern unter Windows Server 2008 oder Windows Server 2008 R2 verwendet werden.

Prozedur

1. Öffnen Sie **Servermanager**.

2. Navigieren Sie zu **Funktionen** > **Funktionen hinzufügen**.

3. Markieren Sie **SMTP-Server**.

   Das Fenster **Für SMTP-Server erforderliche Rollendienste und -funktionen hinzufügen** wird angezeigt.

4. Klicken Sie auf **Erforderliche Rollendienste hinzufügen**.

5. Klicken Sie auf **Weiter**, **Weiter** und anschließend auf **Installieren**.

   Die Webserver-IIS und der SMTP-Server werden installiert

6. Klicken Sie auf **Schließen**.

7. Navigieren Sie zu **Start** > **Verwaltungstools** > **Internet Information Services (IIS) 6.0 Manager**.

   IIS 6.0 Manager wird geöffnet

8. Erweitern Sie **Servername (lokales Gerät)**.

9. Klicken Sie mit der rechten Maustaste auf **[Virtueller SMTP-Server Nr. 1]** und klicken Sie auf **Eigenschaften**.



Hinweis

Markieren Sie zur künftigen Fehlerbehebung die Option **Protokollierung aktivieren**.

10. Navigieren Sie zu **Zugreifen** > **Verbindung...** und wählen Sie **Nur die folgende Liste** aus. Klicken Sie dann auf **Hinzufügen...**.

11. Geben Sie `127.0.0.1` unter **IP-Adresse** an, und klicken Sie auf **OK**.



Hinweis

Wiederholen Sie den Vorgang, um alle IP-Adressen auf dem lokalen Server anzugeben.

12. Klicken Sie auf **OK**.

13. Navigieren Sie zu **Übertragung** > **Erweitert...** und geben Sie die **Maskierte Domäne** in folgendem Format ein: **`psproxy.<Ihre Domäne>.<com/org>`**.

14. Klicken Sie zweimal auf **OK**, um das Fenster **Eigenschaften des virtuellen SMTP-Servers Nr. 1** zu schließen.

15. Navigieren Sie zu **Unternehmensrichtlinien** > **PolicyServer** > **PDA** > **E-Mail**.

16. Öffnen Sie **SMTP-Servername**, geben Sie 127.0.0.1 an und klicken Sie auf **Übernehmen**.

Erweiterten Standort konfigurieren

Erstellen Sie für optimale Ergebnisse einen SPF-DNS-Eintrag (Sender Policy Framework). Informationen zum Erstellen eines SPF-Datensatzes in anderen DNS-Servern (BIND) finden Sie in der Dokumentation des Herstellers.

Prozedur

1. Öffnen Sie **DNS-Management-Konsole** auf einem Windows DNS-Server.

2. Klicken Sie auf die Forward-Lookup-Zone für Domänen und wählen Sie **Andere neue Datensätze** aus.

3. Führen Sie einen Bildlauf nach unten durch und wählen Sie **TEXT (TXT)** aus.

4. Lassen Sie **Name des Datensatzes** leer und geben Sie Folgendes an:

```
v=spf1 ip4:<Ihre externe PolicyServer-IP> -all
```

5. Klicken Sie auf **OK**.

Berichte

PolicyServer zeichnet Systemaktivitäten (an Richtlinien vorgenommene Änderungen, erfolgreiche Authentifizierungsverusche, aufgrund von nicht erfolgreichen Anmeldeversuchen gesperrte Geräte) auf und verwaltet diese Datensätze als Protokollereignisse. Administratoren können Berichte bei Bedarf oder zeitgesteuert generieren.

PolicyServer verfügt über eine Vielzahl an integrierten Berichten, um den Status der Geräteverschlüsselung, die Aktivität von Benutzern oder Geräten und die PolicyServer Integrität zu überprüfen.



Hinweis

Nur Administratoren des Unternehmens können Berichte verwenden.

Berichtoptionen

Verschiedene Berichte haben verschiedene Optionen. Klicken Sie mit der rechten Maustaste auf einen Bericht, um die Optionen anzuzeigen.

TABELLE 8-1. Optionen für Berichte

BERICHTOPTIONEN	OPTIONSBESCHREIBUNG
Löschen	Entfernt alle im Ergebnisfenster angezeigten Informationen, löscht diese aber nicht.

Berichtoptionen	Optionsbeschreibung
Fehler anzeigen	Zeigen Sie eine Beschreibung des Fehlers an, der dazu geführt hat, dass der Bericht ungültig wurde. Diese Option ist nur für Administratoren verfügbar.
Bericht anzeigen	Zeigen Sie den Bericht an. Diese Option ist nur für Administratoren verfügbar.
Nächste Seite	Wechseln Sie zur nächsten Seite der Suchelemente.
Vorherige Seite	Wechseln Sie zur vorherigen Seite der Suchelemente.
Aktualisieren	Aktualisieren Sie den Status eines übermittelten Berichts.
Bericht entfernen	Löscht den Bericht.
Bericht planen	Konfigurieren Sie einen Zeitplan für den Bericht zur Ausführung an einem bestimmten Tag oder zu einer bestimmten Uhrzeit.
Bericht übermitteln	Generieren Sie den ausgewählten Bericht.

Berichtssymbole

Tabelle 8-2. Berichtssymbole

Symbol	Beschreibung
	Standardberichte können je nach Bedarf übermittelt werden, um Statistiken und andere Nutzungsmetriken anzuzeigen.
	Alarmberichte werden verwendet, um Administratoren über potenzielle Sicherheitsprobleme zu unterrichten.

Berichttypen

Berichte dienen dazu, Informationen zu Protokollen einfach verständlich zu machen.

Ausführen von Standardberichten

Standardberichte können je nach Bedarf übermittelt werden. Berichtfunktionen sind nur für Administratoren des Unternehmens zugänglich.

Prozedur

1. Klicken Sie auf den gewünschten Bericht und wählen Sie **Bericht übermitteln** aus.
2. Geben Sie die Berichtsparameter an (falls erforderlich) und klicken Sie auf **Anwenden** .
3. Um den Bericht anzuzeigen, navigieren Sie zu **Unternehmen - Berichte** > **Unternehmen - Übermittelte Berichte**.

Standardberichte

TABELLE 8-3. Liste mit Standardberichten

NAME DES BERICHTS	BESCHREIBUNG
Geräteverschlüsselungsstatus	Listet den Verschlüssellungsstatus für alle Geräte in einem Unternehmen in einem Bericht auf.
Gerätebetriebssysteme und Anzahl	Meldet alle Gerätebetriebssysteme und die Anzahl für jedes System.
Geräteversion und Anzahl	Meldet alle Full Disk Encryption Versionen und die Anzahl für jede Version.
Geräte nach letztem Synchronisierungsdatum	Meldet alle Geräte, die in den letzten x Tagen mit dem PolicyServer synchronisiert wurden.
Nicht kommunizierende Geräte	Meldet die Geräte, die seit x Tagen nicht mit PolicyServer kommuniziert haben.
Geräte mit zuletzt angemeldetem Benutzer	Meldet alle Geräte und den letzten Benutzer, der sich authentifiziert hat.

Name des Berichts	Beschreibung
Verfügbare Unternehmenslizenzen	Meldet die in der Lizenz verbleibenden Tage für die verfügbaren Geräte und Benutzer sowie die Anzahl der Geräte und Benutzer.
Benutzeraktivität im Unternehmen	Meldet die Gesamtzahl der Geräte und Benutzer sowie die MMC-Benutzerzählung im Zusammenhang mit der Geräteaktivität.
Nicht vollständig verschlüsselte Full Disk Encryption Geräte	Meldet alle Geräte in den letzten x Tagen, die mit der Verschlüsselung begonnen, diese aber nicht abgeschlossen haben.
Benutzeraktivität nach Tag	Meldet die Benutzeraktivität innerhalb von x Tagen für den angegebenen Benutzer.
Hinzugefügte Benutzer	Meldet alle Benutzer, die in den letzten x Tagen hinzugefügt wurden.
Benutzer, die sich nie an einem Gerät angemeldet haben	Meldet alle Benutzer, die sich bei einem Gerät authentifiziert haben.

Ausführen von Alarmberichten

Berichtfunktionen sind nur für Administratoren des Unternehmens zugänglich.

Um den Bericht anzuzeigen, navigieren Sie zu **Unternehmen - Berichte** > **Unternehmen - Übermittelte Berichte**.

Prozedur

1. Klicken Sie auf den gewünschten Bericht und wählen Sie **Warnungen konfigurieren** aus.

   Das Fenster **Warnungskonfiguration** wird angezeigt.

2. Geben Sie die **SMTP-Serveradresse** und den **Absender** ein, die die ausgehende E-Mail verarbeiten.

3. Klicken Sie auf **Übernehmen**.

4. Klicken Sie auf den gewünschten Bericht und wählen Sie **Warnung übermitteln** aus.

Alarmberichte

TABELLE 8-4. Liste mit Alarmberichten

ALARMNAME	BESCHREIBUNG
Aufeinanderfolgende fehlgeschlagene Anmeldeversuche auf einem einzelnen Gerät	Es wird eine Warnung gesendet, wenn mehrere aufeinanderfolgende Authentifizierungsversuche bei einem einzelnen Gerät fehlgeschlagen sind.
Protokollintegrität	Es wird eine Warnung gesendet, wenn es Anhaltspunkte dafür gibt, dass die PolicyServer Protokolle manipuliert wurden.
Richtlinienmanipulation	Es wird eine Warnung gesendet, wenn PolicyServer erkennt, dass Richtlinien manipuliert wurden.
Durchgesetzte primäre und sekundäre Aktion	Es wird eine Warnung gesendet, wenn PolicyServer nicht verbunden ist und die primäre oder sekundäre Aktion durchgesetzt wurde.

Anzeigen von Berichten

Berichtfunktionen sind nur für Administratoren des Unternehmens zugänglich.

Prozedur

1. Navigieren Sie zu **Unternehmen - Berichte** > **Unternehmen - Übermittelte Berichte**.

2. Klicken Sie auf den gewünschten Bericht und wählen Sie **Bericht anzeigen** aus.

   Der Bericht wird angezeigt.



Hinweis

Um den Bericht zu exportieren, klicken Sie auf das **Speichersymbol** und wählen Sie **Excel** oder **Acrobat (PDF)-Datei** aus.

Zeitgesteuerte Berichte

Mit diesen Schritten können Berichte an einem bestimmten Datum und zu einer bestimmten Uhrzeit ausgeführt werden.

Prozedur

1. Öffnen Sie **Unternehmen - Berichte**.
2. Klicken Sie auf den gewünschten Bericht und wählen Sie **Bericht planen** aus.

   Das Fenster **Berichtsparameter** wird angezeigt.
3. Geben Sie die Berichtsparameter an und klicken Sie auf **Anwenden**.

   Das Fenster **Berichtsplanung** wird angezeigt.
4. Geben Sie das Berichtsintervall sowie das Datum und die Uhrzeit an und klicken Sie auf **Anwenden**.

   So zeigen Sie geplante Berichte an:
5. Navigieren Sie zu **Unternehmen - Berichte** > **Unternehmen - Zeitgesteuerte Berichte**.

Anzeigen von Berichtsfehlern

Es kann vorkommen, dass ein Bericht aufgrund eines Fehlers nicht ordnungsgemäß ausgeführt wird. Führen Sie diese Schritte aus, um den Fehler anzuzeigen.

Prozedur

1. Navigieren Sie zu **Unternehmen - Berichte** > **Unternehmen - Übermittelte Berichte**.
2. Klicken Sie mit der rechten Maustaste auf den Bericht mit einem Fehler und wählen Sie **Fehler anzeigen** aus.

   Die Berichtsfehlermeldung wird angezeigt.



Kapitel 9

Unterstützung erhalten

Je nach dem, welche Art von Support benötigt wird, gibt es verschiedene Möglichkeiten, Hilfe zu erhalten.

Dieses Kapitel umfasst folgende Themen:

- *Trend Community auf Seite 9-2*
- *Support-Portal auf Seite 9-2*
- *Kontaktaufnahme mit dem technischen Support auf Seite 9-3*
- *TrendLabs auf Seite 9-4*

Trend Community

Hier erhalten Sie Hilfe, können Erfahrungen austauschen, Fragen stellen und Sicherheitsprobleme mit anderen Benutzern, Enthusiasten und Sicherheitsexperten diskutieren.

http://community.trendmicro.com/

Support-Portal

Über das Trend Micro Support-Portal können Sie rund um die Uhr auf Tausende von hilfreichen und einfach zu nutzenden Lösungsvorschlägen zu technischen Problemen mit Trend Micro Produkten und Diensten zugreifen. Täglich werden neue Lösungen hinzugefügt.

Prozedur

1. Gehen Sie zu http://esupport.trendmicro.com.
2. Wählen Sie ein Produkt oder einen Service aus dem entsprechenden Dropdown-Menü aus, und geben Sie weitere verwandte Informationen an, wenn Sie dazu aufgefordert werden.

   Die Produktseite für den Technischen Support wird angezeigt.
3. Geben Sie Suchkriterien an, z. B. eine Fehlermeldung, und klicken Sie anschließend auf das Suchsymbol.

   Eine Liste mit Lösungen wird angezeigt.
4. Wenn in der Liste keine Lösung für Ihr Problem enthalten ist, übermitteln Sie Ihr Problem als Fall. Ein Support-Mitarbeiter von Trend Micro wird sich dann um das Problem kümmern. Die Reaktionszeit beträgt in der Regel maximal 24 Stunden.

   Übermitteln Sie einen Support-Fall online unter:

   http://esupport.trendmicro.com/srf/SRFMain.aspx

Kontaktaufnahme mit dem technischen Support

Bei allen Produktlizenzen erhalten Sie ein Jahr lang technischen Support, Pattern-Downloads und Produkt/Service-Updates. Wenn Sie die Lizenz nach Ablauf des Jahres verlängern, erhalten Sie weiterhin Support von Trend Micro.

Anschriften/Telefonnummern weltweit

```
Weltweite Kontaktadressen für den asiatisch-pazifischen Raum, Australien
http://www.trendmicro.de/ueber-uns/kontakt/index.html
```

- Auf der folgenden Website finden Sie eine Liste unserer weltweiten Support-Büros: http://www.trendmicro.com/us/about-us/contact/index.html
- Auf dieser Website finden Sie die neuesten Dokumentationen von Trend Micro: http://docs.trendmicro.com/de-de/home.aspx

Probleme schneller lösen

Um das Lösen eines Problems zu beschleunigen, halten Sie die folgenden Informationen bereit:

- Schritte, um das Problem nachvollziehen zu können
- Informationen zu Gerät oder Netzwerk
- Marke und Modell des Computers sowie weitere, an den Endpunkt angeschlossene Hardware
- Größe des Arbeitsspeichers und des freien Festplattenspeichers
- Version und Service Pack des verwendeten Betriebssystems
- Endpunkt-Clientversion
- Seriennummer oder Aktivierungscode
- Ausführliche Beschreibung der Installationsumgebung

- Genauer Wortlaut eventueller Fehlermeldungen

TrendLabs

TrendLabs ist ein weltweites Netzwerk aus Forschungs-, Entwicklungs- und Lösungszentren, das rund um die Uhr Bedrohungen überwacht, Präventionsstrategien entwickelt sowie rasche und kontinuierliche Lösungen bereitstellt. TrendLabs bildet die Grundlage der Trend Micro Service-Infrastruktur und beschäftigt mehrere hundert Mitarbeiter und zertifizierte Support-Experten, die sich um die vielfältigen Anfragen zu Produkten und technischem Support kümmern.

TrendLabs überwacht die weltweite Bedrohungslage und liefert wirksame Sicherheitsmaßnahmen für die Erkennung, Vermeidung und Beseitigung von Angriffen. Die Kunden profitieren von diesen täglichen Bemühungen in Form von häufigen Viren-Pattern-Updates und Erweiterungen der Scan Engine.

Weitere Informationen über TrendLabs finden Sie unter:

http://cloudsecurity.trendmicro.com/us/technology-innovation/experts/index.html#trendlabs



Anhang A

PolicyServer Nachrichten-IDs

In diesem Anhang werden die verschiedenen PolicyServer Nachrichten-IDs und ihre Bedeutung aufgeführt.

TABELLE A-1. PolicyServer Nachrichten-IDs

KATEGORIE	NACHRICHTEN-ID	BESCHREIBUNG	PRODUKTE
Administratorwarnungen	100002	Gerät wird identifiziert	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	100003	Sicherheitsverstoß	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	100007	Kritischer Schweregrad	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer

Kategorie	Nachrichten-ID	Beschreibung	Produkte
Administratorwarnungen	100019	Ändern der Richtlinie fehlgeschlagen	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	100045	Nicht unterstützte Konfiguration	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	100046	Unternehmenspool erstellt	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	100047	Unternehmenspool gelöscht	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	100048	Unternehmenspool geändert	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	100049	Admin-Benutzer auf Grund zu vieler fehlgeschlagener Anmeldungen gesperrt.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	100052	Integritätsprüfung des Richtlinienwerts fehlgeschlagen	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer

KATEGORIE	NACHRICHTEN-ID	BESCHREIBUNG	PRODUKTE
Administratorwarnungen	100053	Richtlinienanforderung auf Grund fehlgeschlagener Richtlinienintegritätsprüfung abgebrochen.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	100054	Dateianforderung auf Grund fehlgeschlagener Richtlinienintegritätsprüfung abgebrochen.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	100055	Admin-Authentifizierung erfolgreich	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	100056	Admin-Authentifizierung fehlgeschlagen	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	100062	Admin-Kennwort zurückgesetzt	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	100463	Benutzer kann nicht entfernt werden. Versuchen Sie es erneut.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer

KATEGORIE	NACHRICHTEN-ID	BESCHREIBUNG	PRODUKTE
Administratorwarnungen	100464	Benutzer kann nicht deaktiviert werden. Versuchen Sie es erneut.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	100470	Selbsthilfe-Kennwort kann nicht geändert werden. Eine Antwort auf eine der persönlichen Herausforderungsfragen war falsch.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	102000	Unternehmen hinzugefügt	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	102001	Unternehmen gelöscht	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Administratorwarnungen	102002	Unternehmen geändert	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer

Kategorie	Nachrichten-ID	Beschreibung	Produkte
Administratorwarnungen	102003	Die Anzahl der Benutzer hat das unter dieser Lizenz zulässige Maximum überschritten. Verringern Sie die Anzahl der vorhandenen Benutzer, um dieses Benutzerkonto wiederherzustellen.	PolicyServer
Administratorwarnungen	200000	Administrator hat Richtlinie aktualisiert	PolicyServer
Administratorwarnungen	200001	Administrator hat Richtlinie hinzugefügt	PolicyServer
Administratorwarnungen	200002	Administrator hat Richtlinie gelöscht	PolicyServer
Administratorwarnungen	200003	Administrator hat Richtlinie aktiviert	PolicyServer
Administratorwarnungen	200004	Administrator hat Richtlinie deaktiviert	PolicyServer
Administratorwarnungen	200100	Administrator hat Benutzer hinzugefügt	PolicyServer
Administratorwarnungen	200101	Administrator hat Benutzer gelöscht	PolicyServer
Administratorwarnungen	200102	Administrator hat Benutzer aktualisiert	PolicyServer
Administratorwarnungen	200103	Administrator hat Benutzer zu Gruppe hinzugefügt	PolicyServer

KATEGORIE	NACHRICHTEN-ID	BESCHREIBUNG	PRODUKTE
Administratorwarnungen	200104	Administrator hat Benutzer von Gruppe entfernt	PolicyServer
Administratorwarnungen	200200	Benutzer hinzugefügt	PolicyServer
Administratorwarnungen	200201	Benutzer gelöscht	PolicyServer
Administratorwarnungen	200202	Benutzer zu Gruppe hinzugefügt	PolicyServer
Administratorwarnungen	200203	Benutzer von Gruppe entfernt	PolicyServer
Administratorwarnungen	200204	Benutzer aktualisiert	PolicyServer
Administratorwarnungen	200300	Administrator hat Gerät gelöscht	PolicyServer
Administratorwarnungen	200301	Administrator hat Gerät zu Gruppe hinzugefügt	PolicyServer
Administratorwarnungen	200302	Administrator hat Gerät von Gruppe entfernt	PolicyServer
Administratorwarnungen	200500	Administrator hat Gruppe hinzugefügt	PolicyServer
Administratorwarnungen	200501	Administrator hat Gruppe gelöscht	PolicyServer
Administratorwarnungen	200502	Administrator hat Gruppe aktualisiert	PolicyServer
Administratorwarnungen	200503	Administrator hat Gruppe kopiert/ eingefügt	PolicyServer

Kategorie	Nachrichten-ID	Beschreibung	Produkte
Administratorwarnungen	200600	Update des PolicyServer angewendet.	PolicyServer
Administratorwarnungen	200602	Benutzer zu Gerät hinzugefügt	PolicyServer
Administratorwarnungen	200603	Benutzer von Gerät entfernt	PolicyServer
Administratorwarnungen	200700	Ereignis ausgeführt	PolicyServer
Administratorwarnungen	200701	Ereignisausführung fehlgeschlagen	PolicyServer
Administratorwarnungen	200800	Ereignis installiert	PolicyServer
Administratorwarnungen	200801	Installation des Ereignisses fehlgeschlagen	PolicyServer
Administratorwarnungen	700012	Angemeldeter Administrator verwendet Einmalkennwort	FileArmor SP6 oder früher
Administratorwarnungen	700013	Angemeldeter Administrator verwendet festes Kennwort	FileArmor SP6 oder früher
Administratorwarnungen	700014	Angemeldeter Administrator verwendet Smartcard	FileArmor SP6 oder früher
Administratorwarnungen	700017	Angemeldeter Administrator verwendet Remote-Authentifizierung	FileArmor SP6 oder früher

KATEGORIE	NACHRICHTEN-ID	BESCHREIBUNG	PRODUKTE
Administratorwarnungen	700030	Anmelden des Administrators mit Einmalkennwort ist fehlgeschlagen	FileArmor SP6 oder früher
Administratorwarnungen	700031	Anmelden des Administrators mit festem Kennwort ist fehlgeschlagen	FileArmor SP6 oder früher
Administratorwarnungen	700032	Anmelden des Administrators mit Smartcard ist fehlgeschlagen	FileArmor SP6 oder früher
Administratorwarnungen	700035	Anmelden des Administrators mit der Remote-Authentifizierung ist fehlgeschlagen	FileArmor SP6 oder früher
Administratorwarnungen	900100	Angemeldeter Administrator verwendet Einmalkennwort.	KeyArmor
Administratorwarnungen	900101	Angemeldeter Administrator verwendet festes Kennwort.	KeyArmor
Administratorwarnungen	900102	Angemeldeter Administrator verwendet Smartcard.	KeyArmor
Administratorwarnungen	900103	Angemeldeter Administrator verwendet Domänenauthentifizierung.	KeyArmor

KATEGORIE	NACHRICHTEN-ID	BESCHREIBUNG	PRODUKTE
Administratorwarnunge n	900104	Angemeldeter Administrator verwendet Remote-Authentifizierung.	KeyArmor
Administratorwarnunge n	900105	Angemeldeter Administrator verwendet ColorCode-Authentifizierung.	KeyArmor
Administratorwarnunge n	900106	Angemeldeter Administrator verwendet PIN.	KeyArmor
Administratorwarnunge n	900107	Angemeldeter Administrator verwendet OCSP.	KeyArmor
Administratorwarnunge n	900250	Anmelden des Administrators mit Einmalkennwort ist fehlgeschlagen.	KeyArmor
Administratorwarnunge n	900251	Anmelden des Administrators mit festem Kennwort ist fehlgeschlagen.	KeyArmor
Administratorwarnunge n	900252	Anmelden des Administrators mit Smartcard ist fehlgeschlagen.	KeyArmor
Administratorwarnunge n	900253	Anmelden des Administrators mit Domänenauthentifiz ierung ist fehlgeschlagen.	KeyArmor

KATEGORIE	NACHRICHTEN-ID	BESCHREIBUNG	PRODUKTE
Administratorwarnungen	900254	Anmelden des Administrators mit Remote-Authentifizierung ist fehlgeschlagen.	KeyArmor
Administratorwarnungen	900255	Anmelden des Administrators mit ColorCode-Authentifizierung ist fehlgeschlagen.	KeyArmor
Administratorwarnungen	900256	Anmelden des Administrators mit PIN ist fehlgeschlagen.	KeyArmor
Administratorwarnungen	900257	Anmelden des Administrators mit OCSP ist fehlgeschlagen.	KeyArmor
Administratorwarnungen	900300	Anmelden des Administrators mit der Remote-Authentifizierung ist fehlgeschlagen	KeyArmor
Administratorwarnungen	901000	Administrator hat eine Datei umbenannt	KeyArmor
Administratorwarnungen	901001	Administrator hat eine Datei geändert	KeyArmor
Administratorwarnungen	901002	Administrator hat eine Datei gelöscht	KeyArmor
Administratorwarnungen	901003	Administrator hat eine Datei erstellt	KeyArmor

Kategorie	Nachrichten-ID	Beschreibung	Produkte
Audit-Protokoll-Warnungen	100015	Protokollmeldung	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Audit-Protokoll-Warnungen	103000	Audit-Protokoll-Verbindung geöffnet	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Audit-Protokoll-Warnungen	103001	Audit-Protokoll-Verbindung geschlossen	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Audit-Protokoll-Warnungen	103100	Audit-Protokoll-Datensatz fehlt	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Audit-Protokoll-Warnungen	103101	Keine Integrität bei Audit-Protokoll-Datensatz	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Audit-Protokoll-Warnungen	103102	Integrität von Audit-Protokoll-Datensatz gefährdet	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Audit-Protokoll-Warnungen	103103	Validierung der Integrität des Audit-Protokoll-Datensatzes gestartet	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer

Kategorie	Nachrichten-ID	Beschreibung	Produkte
Audit-Protokoll-Warnungen	104003	Authentifizierungsmethode auf Smartcard festgelegt.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Audit-Protokoll-Warnungen	904008	Protokollwarnung kann nicht gesendet werden	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Authentifiziererwarnungen	700006	Angemeldeter Authentifizierer verwendet Einmalkennwort	FileArmor SP6 oder früher
Authentifiziererwarnungen	700007	Angemeldeter Authentifizierer verwendet festes Kennwort	FileArmor SP6 oder früher
Authentifiziererwarnungen	700008	Angemeldeter Authentifizierer verwendet Smartcard	FileArmor SP6 oder früher
Authentifiziererwarnungen	700009	Angemeldeter Authentifizierer verwendet Windows Anmeldedaten	FileArmor SP6 oder früher
Authentifiziererwarnungen	700011	Angemeldeter Authentifizierer verwendet Remote-Authentifizierung	FileArmor SP6 oder früher
Authentifiziererwarnungen	700024	Anmelden des Authentifizierers mit Einmalkennwort ist fehlgeschlagen	FileArmor SP6 oder früher

Kategorie	Nachrichten-ID	Beschreibung	Produkte
Authentifiziererwarnungen	700025	Anmelden des Authentifizierers mit festem Kennwort ist fehlgeschlagen	FileArmor SP6 oder früher
Authentifiziererwarnungen	700026	Anmelden des Authentifizierers mit Smartcard ist fehlgeschlagen	FileArmor SP6 oder früher
Authentifiziererwarnungen	700027	Anmelden des Authentifizierers mit Windows Anmeldedaten ist fehlgeschlagen	FileArmor SP6 oder früher
Authentifiziererwarnungen	700029	Anmelden des Authentifizierers mit der Remote-Authentifizierung ist fehlgeschlagen	FileArmor SP6 oder früher
Authentifiziererwarnungen	900050	Angemeldeter Authentifizierer verwendet Einmalkennwort.	KeyArmor
Authentifiziererwarnungen	900051	Angemeldeter Authentifizierer verwendet festes Kennwort.	KeyArmor
Authentifiziererwarnungen	900052	Angemeldeter Authentifizierer verwendet Smartcard.	KeyArmor
Authentifiziererwarnungen	900053	Angemeldeter Authentifizierer verwendet Domänenauthentifizierung.	KeyArmor

KATEGORIE	NACHRICHTEN-ID	BESCHREIBUNG	PRODUKTE
Authentifiziererwarnungen	900054	Angemeldeter Authentifizierer verwendet Remote-Authentifizierung.	KeyArmor
Authentifiziererwarnungen	900055	Angemeldeter Authentifizierer verwendet ColorCode-Authentifizierung.	KeyArmor
Authentifiziererwarnungen	900056	Angemeldeter Authentifizierer verwendet PIN.	KeyArmor
Authentifiziererwarnungen	900057	Angemeldeter Authentifizierer verwendet OCSP.	KeyArmor
Authentifiziererwarnungen	900161	Anmelden des Benutzers mit Selbsthilfe ist fehlgeschlagen.	KeyArmor
Authentifiziererwarnungen	900200	Anmelden des Authentifizierers mit Einmalkennwort ist fehlgeschlagen.	KeyArmor
Authentifiziererwarnungen	900201	Anmelden des Authentifizierers mit festem Kennwort ist fehlgeschlagen.	KeyArmor
Authentifiziererwarnungen	900202	Anmelden des Authentifizierers mit Smartcard ist fehlgeschlagen.	KeyArmor

Kategorie	Nachrichten-ID	Beschreibung	Produkte
Authentifiziererwarnungen	900203	Anmelden des Authentifizierers mit Domänenauthentifizierung ist fehlgeschlagen.	KeyArmor
Authentifiziererwarnungen	900204	Anmelden des Authentifizierers mit Remote-Authentifizierung ist fehlgeschlagen.	KeyArmor
Authentifiziererwarnungen	900205	Anmelden des Authentifizierers mit ColorCode-Authentifizierung ist fehlgeschlagen.	KeyArmor
Authentifiziererwarnungen	900206	Anmelden des Authentifizierers mit PIN ist fehlgeschlagen.	KeyArmor
Authentifiziererwarnungen	900207	Anmelden des Authentifizierers mit OCSP ist fehlgeschlagen.	KeyArmor
Authentifiziererwarnungen	902000	Authentifizierer hat eine Datei umbenannt	KeyArmor
Authentifiziererwarnungen	902001	Authentifizierer hat eine Datei geändert	KeyArmor
Authentifiziererwarnungen	902002	Authentifizierer hat eine Datei gelöscht	KeyArmor
Authentifiziererwarnungen	902003	Authentifizierer hat eine Datei erstellt	KeyArmor

Kategorie	Nachrichten-ID	Beschreibung	Produkte
Zertifikatswarnungen	104008	Zertifikat abgelaufen.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Gerätewarnungen	100001	Authentifizierung für die Synchronisierung zwischen PDA und Desktop war nicht erfolgreich. Es wurde für diesen PDA keine Geräte-ID gefunden.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Gerätewarnungen	100012	Gerät befindet sich nicht in seiner eigenen Kennwortauthentifizierungsdatei. PAF beschädigt?	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Gerätewarnungen	100044	Aktion zum Sperren von Geräten empfangen	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Gerätewarnungen	100071	Auslöschen des Geräts bestätigt	KeyArmor
Gerätewarnungen	100072	Gerätesperre bestätigt	KeyArmor
Gerätewarnungen	100100	Installation gestartet	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor

KATEGORIE	NACHRICHTEN-ID	BESCHREIBUNG	PRODUKTE
Gerätewarnungen	100101	Installation abgeschlossen	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor
Gerätewarnungen	100462	Verbindung mit PolicyServer nicht möglich.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Gerätewarnungen	101001	Die Netzwerkverbindung funktioniert nicht. Die Richtliniendateien können nicht vom PolicyServer abgerufen werden.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Gerätewarnungen	101002	Beschädigte PAF-Datei (DAFolder.xml)	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Gerätewarnungen	105000	Richtlinien können nicht mit Client synchronisiert werden. Überprüfen Sie, ob eine Netzwerkverbindung vorhanden ist, und versuchen Sie es erneut.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Gerätewarnungen	200400	Gerät hinzugefügt	PolicyServer
Gerätewarnungen	200401	Gerät gelöscht	PolicyServer
Gerätewarnungen	200402	Gerät zu Gruppe hinzugefügt	PolicyServer

Kategorie	Nachrichten-ID	Beschreibung	Produkte
Gerätewarnungen	200403	Gerät von Gruppe entfernt	PolicyServer
Gerätewarnungen	200404	Gerät geändert	PolicyServer
Gerätewarnungen	200405	Gerätestatus aktualisiert	PolicyServer
Gerätewarnungen	200406	Gerätestatus zurückgesetzt	PolicyServer
Gerätewarnungen	200407	Auslöschen des Geräts ausgelöst	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Gerätewarnungen	200408	Gerätesperre ausgestellt	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Gerätewarnungen	200409	Gerät synchronisiert	PolicyServer
Gerätewarnungen	904012	Der Benutzer darf kein neues Gerät registrieren.	PolicyServer
Gerätewarnungen	1000052	Deinstallation des Produkts	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor
Gerätewarnungen	1000053	Deinstallation des Produkts von Richtlinie verweigert	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor

KATEGORIE	NACHRICHTEN-ID	BESCHREIBUNG	PRODUKTE
Fehlerwarnungen	100005	Allgemeiner Fehler	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Fehlerwarnungen	100006	Anwendungsfehler	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Warnungen bei FileArmor Aktivität	700000	Angemeldeter Benutzer verwendet Einmalkennwort	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	700001	Angemeldeter Benutzer verwendet festes Kennwort	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	700002	Angemeldeter Benutzer verwendet Smartcard	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	700003	Angemeldeter Benutzer verwendet Windows Anmeldedaten	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	700005	Angemeldeter Benutzer verwendet Remote-Authentifizierung	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	700015	Angemeldeter Administrator verwendet Windows Anmeldedaten	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	700018	Anmelden des Benutzers mit Einmalkennwort ist fehlgeschlagen	FileArmor SP6 oder früher

Kategorie	Nachrichten-ID	Beschreibung	Produkte
Warnungen bei FileArmor Aktivität	700019	Anmelden des Benutzers mit festem Kennwort ist fehlgeschlagen	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	700020	Anmelden des Benutzers mit Smartcard ist fehlgeschlagen	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	700021	Anmelden des Benutzers mit Windows Anmeldedaten ist fehlgeschlagen	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	700023	Benutzer konnte sich mit der Remote-Authentifizierung nicht anmelden	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	700033	Anmelden des Administrators mit Windows Anmeldedaten ist fehlgeschlagen	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	700036	Anzahl fehlgeschlagener Anmeldeversuche überschritten	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	701000	Verschlüsselte Datei unter Verwendung eines Benutzerschlüssels	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	701001	Verschlüsselte Datei unter Verwendung eines Gruppenschlüssels	FileArmor SP6 oder früher

Kategorie	Nachrichten-ID	Beschreibung	Produkte
Warnungen bei FileArmor Aktivität	701002	Verschlüsselte Datei unter Verwendung eines statischen Kennworts	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	701003	Selbstextrahierende, verschlüsselte Datei, die unter Verwendung eines statischen Kennworts erstellt wurde.	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	701004	Verschlüsselte Datei unter Verwendung eines Zertifikats	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	701005	Selbstextrahierende, verschlüsselte Datei, die unter Verwendung eines Zertifikats erstellt wurde.	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	701006	Verschlüsselte Datei unter Verwendung eines CD/DVD-Brennvorgangs	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	701007	Verschlüsseltes Verzeichnis unter Verwendung eines Gruppenschlüssels	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	701008	Verschlüsseltes Verzeichnis unter Verwendung eines statischen Kennworts	FileArmor SP6 oder früher

Kategorie	Nachrichten-ID	Beschreibung	Produkte
Warnungen bei FileArmor Aktivität	701009	Selbstextrahierendes, verschlüsseltes Verzeichnis, das unter Verwendung eines statischen Kennworts erstellt wurde.	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	701010	Verschlüsseltes Verzeichnis unter Verwendung eines Zertifikats	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	701011	Selbstextrahierendes, verschlüsseltes Verzeichnis, das unter Verwendung eines Zertifikats erstellt wurde.	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	701012	Verschlüsselter Ordner unter Verwendung eines CD/DVD-Brennvorgangs	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	701015	Wechselmedium wurde vollständig verschlüsselt	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	701016	Wechselmedium gesperrt	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	701017	Auf Wechselmedium wurden Ordner erstellt und einbezogen	FileArmor SP6 oder früher

KATEGORIE	NACHRICHTEN-ID	BESCHREIBUNG	PRODUKTE
Warnungen bei FileArmor Aktivität	701018	Datei verschlüsselt und auf Wechselmedium verschoben.	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	701019	Datei von Wechselmedium gelöscht.	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	703000	Mit FileArmor verschlüsselter Ordner wurde erstellt	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	703001	Ordner wurde erstellt und einbezogen	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	703002	Mit FileArmor verschlüsselter Ordner wurde gelöscht	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	703004	Auf Wechselmedium wurde Ordner erstellt und einbezogen	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	703005	Wechseldatenträger wurde vollständig verschlüsselt	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	703006	Datei in Ordner wurde erstellt	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	703007	Datei in Ordner wurde gelöscht	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	703008	Datei in Ordner wurde geändert	FileArmor SP6 oder früher

Kategorie	Nachrichten-ID	Beschreibung	Produkte
Warnungen bei FileArmor Aktivität	703009	Auf Datei in Ordner wurde zugegriffen	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	703010	Datei in Ordner wurde zuletzt geschrieben	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	703011	Dateigröße in Ordner geändert	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	703015	Ordnerverschlüsselung gestartet	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	703016	Ordnerentschlüsselung gestartet	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	703017	Ordnerverschlüsselung abgeschlossen	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	703018	Ordnerentschlüsselung abgeschlossen	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	703019	Ordnerentschlüsselung läuft	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	703020	Ordnerverschlüsselung läuft	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	704000	FileArmor Dienst gestartet	FileArmor SP6 oder früher
Warnungen bei FileArmor Aktivität	704001	FileArmor Dienst heruntergefahren	FileArmor SP6 oder früher
Warnungen bei Full Disk Encryption	300700	Maximale Größe des Geräteprotokolls erreicht, Ereignisprotokoll wird abgeschnitten.	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	400001	Benutzer hat sich angemeldet.	Full Disk Encryption oder MobileSentinel

KATEGORIE	NACHRICHTEN-ID	BESCHREIBUNG	PRODUKTE
Warnungen bei Full Disk Encryption	400002	Benutzeranmeldung fehlgeschlagen.	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	400003	Geräteentschlüssel ung gestartet.	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	400004	Geräteverschlüssel ung gestartet.	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	400005	Verschlüsselte Partition gemountet.	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	400006	Nativer OS-MBR wiederhergestellt.	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	400007	Anwendungs-MBR wiederhergestellt.	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	400008	Geräteverschlüssel ung abgeschlossen	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	400009	Geräteentschlüssel ung abgeschlossen	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	400010	Geräteverschlüssel ung wird durchgeführt	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	400011	System-MBR beschädigt	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	400012	Preboot-Kernel des Systems gelöscht	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401000	Zugriff auf Wiederherstellungsk onsole	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401009	Fehler bei Wiederherstellungsk onsole	Full Disk Encryption oder MobileSentinel

Kategorie	Nachrichten-ID	Beschreibung	Produkte
Warnungen bei Full Disk Encryption	401010	In-Place-Entschlüsselung gestartet	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401011	In-Place-Entschlüsselung gestoppt	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401012	In-Place-Entschlüsselung abgeschlossen	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401013	Entschlüsselung des Wechseldatenträgers gestartet	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401014	Entschlüsselung des Wechseldatenträgers gestoppt	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401015	Entschlüsselung des Wechseldatenträgers abgeschlossen	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401018	Fehler bei In-Place-Entschlüsselung	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401019	Fehler bei Entschlüsselung des Wechseldatenträgers	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401020	Zugriff auf verschlüsselte Dateien	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401021	Verschlüsselte Dateien geändert	Full Disk Encryption oder MobileSentinel

KATEGORIE	NACHRICHTEN-ID	BESCHREIBUNG	PRODUKTE
Warnungen bei Full Disk Encryption	401022	Verschlüsselte Dateien auf Wechseldatenträger kopiert	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401029	Fehler beim Zugriff auf verschlüsselte Dateien	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401030	Zugriff auf Netzwerkadministrat ion	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401031	PolicyServer Adresse geändert	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401032	PolicyServer Portnummer geändert	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401033	Zu IPv6 gewechselt	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401034	Zu IPv4 gewechselt	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401035	Zur dynamischen IP-Konfiguration gewechselt	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401036	Zur statischen IP-Konfiguration gewechselt	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401037	DHCP-Portnummer geändert	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401038	IP-Adresse geändert	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401039	Netzmaske geändert	Full Disk Encryption oder MobileSentinel

KATEGORIE	NACHRICHTEN-ID	BESCHREIBUNG	PRODUKTE
Warnungen bei Full Disk Encryption	401040	Broadcast-Adresse geändert	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401041	Gateway geändert	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401042	Domänenname geändert	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401043	Domain Name Server geändert	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401049	Fehler bei Netzwerkadministration	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401050	Zugriff auf Benutzeradministration	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401051	Benutzer hinzugefügt	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401052	Benutzer entfernt	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401053	Benutzer geändert	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401069	Fehler bei Benutzeradministration	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401070	Zugriff auf lokal gespeicherte Protokolle	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401079	Fehler bei Zugriff auf lokal gespeicherte Protokolle	Full Disk Encryption oder MobileSentinel

Kategorie	Nachrichten-ID	Beschreibung	Produkte
Warnungen bei Full Disk Encryption	401080	Ursprünglicher MBR wiederhergestellt	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401089	Fehler beim Wiederherstellen des ursprünglichen MBR	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401090	Standarddesign wiederhergestellt	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	401099	Fehler bei Wiederherstellung des Standarddesigns	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	402000	Start der Anwendung	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	402001	Herunterfahren der Anwendung	Full Disk Encryption oder MobileSentinel
Warnungen bei Full Disk Encryption	600001	Preboot-Update war erfolgreich.	Full Disk Encryption
Warnungen bei Full Disk Encryption	600002	Preboot-Update fehlgeschlagen	Full Disk Encryption
Installationswarnungen	100004	Installationsfehler	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Installationswarnungen	100020	Erfolgreiche Installation	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Installationswarnungen	700037	Installation von FileArmor war erfolgreich	FileArmor SP6 oder früher

KATEGORIE	NACHRICHTEN-ID	BESCHREIBUNG	PRODUKTE
Installationswarnungen	700038	Installation von FileArmor war nicht erfolgreich: Unternehmensname ist nicht gültig.	FileArmor SP6 oder früher
Installationswarnungen	700039	Installation von FileArmor war nicht erfolgreich: Benutzername oder Kennwort ist falsch.	FileArmor SP6 oder früher
Warnungen bei KeyArmor Aktivität	100034	Ungültige Registrierungseinst ellung erkannt	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Warnungen bei KeyArmor Aktivität	500000	VirusDefense	KeyArmor
Warnungen bei KeyArmor Aktivität	500001	Objekt gesäubert	KeyArmor
Warnungen bei KeyArmor Aktivität	500002	Objekt desinfiziert	KeyArmor
Warnungen bei KeyArmor Aktivität	500003	Objekt in Quarantäne	KeyArmor
Warnungen bei KeyArmor Aktivität	500004	Objekt gelöscht	KeyArmor
Warnungen bei KeyArmor Aktivität	500005	Virus entdeckt	KeyArmor
Warnungen bei KeyArmor Aktivität	500006	Vollständige Suche gestartet	KeyArmor
Warnungen bei KeyArmor Aktivität	500007	Vollständige Suche abgeschlossen	KeyArmor

Kategorie	Nachrichten-ID	Beschreibung	Produkte
Warnungen bei KeyArmor Aktivität	500008	Objekt verdächtig	KeyArmor
Warnungen bei KeyArmor Aktivität	500009	Objektsuche abgeschlossen	KeyArmor
Warnungen bei KeyArmor Aktivität	500010	Suche auf Wechselmedium angefordert	KeyArmor
Warnungen bei KeyArmor Aktivität	500011	Suche auf Wechselmedium abgeschlossen	KeyArmor
Warnungen bei KeyArmor Aktivität	500012	Suche in Ordner angefordert	KeyArmor
Warnungen bei KeyArmor Aktivität	500013	Suche in Ordner abgeschlossen	KeyArmor
Warnungen bei KeyArmor Aktivität	500014	Zugriff auf Objekt verweigert	KeyArmor
Warnungen bei KeyArmor Aktivität	500015	Objekt beschädigt	KeyArmor
Warnungen bei KeyArmor Aktivität	500016	Objekt sauber	KeyArmor
Warnungen bei KeyArmor Aktivität	500017	Vollständige Suche abgebrochen	KeyArmor
Warnungen bei KeyArmor Aktivität	500018	Suche in Objekt abgebrochen	KeyArmor
Warnungen bei KeyArmor Aktivität	500019	Suche auf Wechselmedium abgebrochen	KeyArmor
Warnungen bei KeyArmor Aktivität	500020	Suche in Ordner abgebrochen	KeyArmor

KATEGORIE	NACHRICHTEN-ID	BESCHREIBUNG	PRODUKTE
Warnungen bei KeyArmor Aktivität	500021	Update gestartet	KeyArmor
Warnungen bei KeyArmor Aktivität	500022	Das Update war nicht erfolgreich. Versuchen Sie es erneut.	KeyArmor
Warnungen bei KeyArmor Aktivität	500023	Update abgebrochen	KeyArmor
Warnungen bei KeyArmor Aktivität	500024	Update erfolgreich.	KeyArmor
Warnungen bei KeyArmor Aktivität	500025	VirusDefense auf dem neuesten Stand	KeyArmor
Warnungen bei KeyArmor Aktivität	500026	PalmVirusDefense	KeyArmor
Warnungen bei KeyArmor Aktivität	500027	Suche in Objekt angefordert	KeyArmor
Warnungen bei KeyArmor Aktivität	500028	PPCVirusDefense	KeyArmor
Warnungen bei KeyArmor Aktivität	900000	Angemeldeter Benutzer verwendet Einmalkennwort.	KeyArmor
Warnungen bei KeyArmor Aktivität	900001	Angemeldeter Benutzer verwendet festes Kennwort.	KeyArmor
Warnungen bei KeyArmor Aktivität	900002	Angemeldeter Benutzer verwendet Smartcard.	KeyArmor
Warnungen bei KeyArmor Aktivität	900003	Angemeldeter Benutzer verwendet Domänenauthentifizierung.	KeyArmor

Kategorie	Nachrichten-ID	Beschreibung	Produkte
Warnungen bei KeyArmor Aktivität	900004	Angemeldeter Benutzer verwendet Remote-Authentifizierung.	KeyArmor
Warnungen bei KeyArmor Aktivität	900005	Angemeldeter Benutzer verwendet ColorCode-Authentifizierung.	KeyArmor
Warnungen bei KeyArmor Aktivität	900006	Angemeldeter Benutzer verwendet PIN.	KeyArmor
Warnungen bei KeyArmor Aktivität	900007	Angemeldeter Benutzer verwendet OCSP	KeyArmor
Warnungen bei KeyArmor Aktivität	900008	Angemeldeter Benutzer verwendet Selbsthilfe.	KeyArmor
Warnungen bei KeyArmor Aktivität	900009	Angemeldeter Benutzer verwendet RSA	KeyArmor
Warnungen bei KeyArmor Aktivität	900150	Anmelden des Benutzers mit Einmalkennwort ist fehlgeschlagen.	KeyArmor
Warnungen bei KeyArmor Aktivität	900151	Anmelden des Benutzers mit festem Kennwort ist fehlgeschlagen.	KeyArmor
Warnungen bei KeyArmor Aktivität	900152	Anmelden des Benutzers mit Smartcard ist fehlgeschlagen.	KeyArmor

KATEGORIE	NACHRICHTEN-ID	BESCHREIBUNG	PRODUKTE
Warnungen bei KeyArmor Aktivität	900153	Anmelden des Benutzers mit Domänenauthentifizierung ist fehlgeschlagen.	KeyArmor
Warnungen bei KeyArmor Aktivität	900154	Anmelden des Benutzers mit Remote-Authentifizierung ist fehlgeschlagen.	KeyArmor
Warnungen bei KeyArmor Aktivität	900155	Anmelden des Benutzers mit ColorCode-Authentifizierung ist fehlgeschlagen.	KeyArmor
Warnungen bei KeyArmor Aktivität	900156	Anmelden des Benutzers mit PIN ist fehlgeschlagen.	KeyArmor
Warnungen bei KeyArmor Aktivität	900157	Anmelden des Benutzers mit OCSP ist fehlgeschlagen.	KeyArmor
Warnungen bei KeyArmor Aktivität	900158	Benutzer wurde nach zu vielen fehlgeschlagenen Anmeldeversuchen gesperrt.	KeyArmor
Warnungen bei KeyArmor Aktivität	900301	Anzahl fehlgeschlagener Anmeldeversuche überschritten	KeyArmor
Warnungen bei KeyArmor Aktivität	900350	Schlüssel per Wipe gelöscht	KeyArmor
Warnungen bei KeyArmor Aktivität	903000	Benutzer hat eine Datei umbenannt	KeyArmor

Kategorie	Nachrichten-ID	Beschreibung	Produkte
Warnungen bei KeyArmor Aktivität	903001	Benutzer hat eine Datei geändert	KeyArmor
Warnungen bei KeyArmor Aktivität	903002	Benutzer hat eine Datei gelöscht	KeyArmor
Warnungen bei KeyArmor Aktivität	903003	Benutzer hat eine Datei erstellt	KeyArmor
Warnungen bei KeyArmor Aktivität	903100	Primäraktion erzwungen, da keine PolicyServer Verbindung besteht.	KeyArmor
Warnungen bei KeyArmor Aktivität	903101	Sekundäraktion erzwungen, da keine PolicyServer Verbindung besteht.	KeyArmor
Warnungen bei KeyArmor Aktivität	903102	Richtlinien-Updates angewendet	KeyArmor
Warnungen bei KeyArmor Aktivität	904000	Infizierte Datei repariert	KeyArmor
Warnungen bei KeyArmor Aktivität	904001	Reparieren der infizierten Datei nicht möglich.	KeyArmor
Warnungen bei KeyArmor Aktivität	904002	Infizierte Datei wird übersprungen, Reparatur wird nicht unterstützt	KeyArmor
Warnungen bei KeyArmor Aktivität	904003	Infizierte Datei gelöscht	KeyArmor
Warnungen bei KeyArmor Aktivität	904004	Löschen der infizierten Datei nicht möglich.	KeyArmor

Kategorie	Nachrichten-ID	Beschreibung	Produkte
Warnungen bei KeyArmor Aktivität	904005	Gerät wird auf Grund infizierter Datei ausgelöscht	KeyArmor
Warnungen bei KeyArmor Aktivität	904006	Fehler beim Auslöschen des Geräts auf Grund infizierter Datei	KeyArmor
Warnungen bei KeyArmor Aktivität	904007	Fallback-Aktion für infizierte Datei wird aufgerufen	KeyArmor
Warnungen bei KeyArmor Aktivität	904010	Antivirus-Dateien aktualisiert	KeyArmor
Warnungen bei KeyArmor Aktivität	904011	Antivirus-Dateien können nicht aktualisiert werden.	KeyArmor
Anmelde-/ Abmeldewarnungen	100013	Fehlgeschlagener Anmeldeversuch	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100014	Erfolgreiche Anmeldung	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100016	Anmeldung nicht möglich. Verwenden Sie die Remote-Authentifizierung, um den PolicyServer Administrator mit einem Herausforderungscode zu versehen.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer

Kategorie	Nachrichten-ID	Beschreibung	Produkte
Anmelde-/ Abmeldewarnungen	100021	Erfolglose ColorCode-Anmeldung	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100022	Erfolglose Anmeldung per festem Kennwort	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100023	Erfolglose PIN-Anmeldung	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100024	Erfolglose X99-Anmeldung	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100028	Erfolgreiche ColorCode-Anmeldung	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100031	Erfolgreiche X9.9-Anmeldung	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100032	Erfolgreiche Remote-Anmeldung	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer

KATEGORIE	NACHRICHTEN-ID	BESCHREIBUNG	PRODUKTE
Anmelde-/ Abmeldewarnungen	100035	Erfolgreiche WebToken-Anmeldung	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100036	Erfolglose WebToken-Anmeldung	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100050	Anmeldung mit festem Kennwort durch Sperre blockiert.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100051	Benutzeranmeldung entsperrt	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100057	LDAP-Benutzerauthentifizierung erfolgreich	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100058	LDAP-Benutzerauthentifizierung fehlgeschlagen	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100059	Änderung des LDAP-Benutzerkennworts erfolgreich	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer

Kategorie	Nachrichten-ID	Beschreibung	Produkte
Anmelde-/ Abmeldewarnungen	100060	Änderung des LDAP-Benutzerkennworts fehlgeschlagen	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100061	Zugriffsanforderung auf Grund fehlgeschlagener Richtlinienintegritäts prüfung abgebrochen.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100070	Erfolgreiche Abmeldung	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100433	Die ColorCodes stimmen nicht überein.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100434	ColorCode kann nicht geändert werden. Der neue ColorCode muss sich vom aktuellen unterscheiden.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100435	ColorCode kann nicht geändert werden. Der neue ColorCode muss die von PolicyServer definierten Mindestanforderung en für die Länge erfüllen.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer

Kategorie	Nachrichten-ID	Beschreibung	Produkte
Anmelde-/ Abmeldewarnungen	100436	ColorCode kann nicht geändert werden. Der neue ColorCode muss sich von allen zuvor verwendeten ColorCodes unterscheiden.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100437	Ändern des ColorCode fehlgeschlagen - Interner Fehler	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100459	X9.9 - Fehler bei Kennwortänderung - Verbindung zu PolicyServer Host nicht möglich	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100460	X9.9 - Fehler bei Kennwortänderung - Leere Seriennummer	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	100461	X9.9 - Fehler bei Kennwortänderung - Interner Fehler	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	101004	Gesperrtes Gerät kann nicht zurückgesetzt werden.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer

KATEGORIE	NACHRICHTEN-ID	BESCHREIBUNG	PRODUKTE
Anmelde-/ Abmeldewarnungen	104000	Smartcard-Anmeldung erfolgreich.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Anmelde-/ Abmeldewarnungen	104001	Smartcard-Anmeldung nicht erfolgreich. Prüfen Sie, ob die Karte ordnungsgemäß eingelegt wurde und die Smartcard-PIN gültig ist.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Mobilgerätewarnung	100037	Palm-Richtliniendatenbank fehlt	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Mobilgerätewarnung	100038	Fehler bei Palm-Verschlüsselung	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Mobilgerätewarnung	100039	PPC - Geräteverschlüsselung geändert	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Mobilgerätewarnung	100040	PPC - Fehler bei Verschlüsselung	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Warnungen bei MobileFirewall-Aktivität	300000	MobileFirewall	MobileFirewall

Kategorie	Nachrichten-ID	Beschreibung	Produkte
Warnungen bei MobileFirewall-Aktivität	300001	DenialOfServiceAtta ck	MobileFirewall
OCSP-Warnungen	104005	OCSP-Zertifikatsstatus gut.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
OCSP-Warnungen	104006	OCSP-Zertifikatsstatus widerrufen.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
OCSP-Warnungen	104007	OCSP-Zertifikatsstatus unbekannt.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
OTA-Warnungen	100041	OTA-Objekt fehlt oder ist beschädigt.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
OTA-Warnungen	100042	OTA-Synchronisierung erfolgreich	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
OTA-Warnungen	100043	OTA-Gerät ausgelöscht	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer

Kategorie	Nachrichten-ID	Beschreibung	Produkte
Kennwortwarnungen	100017	Fehler beim Ändern des Kennworts	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100018	Anzahl der Versuche zur Kennworteingabe überschritten	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100025	Kennwort zurückgesetzt auf 'ColorCode'	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100026	Kennwort zurückgesetzt auf 'Fest'	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100027	Kennwort zurückgesetzt auf PIN	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100029	Erfolgreiche Anmeldung per festem Kennwort	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100030	Erfolgreiche Anmeldung per PIN-Kennwort	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer

KATEGORIE	NACHRICHTEN-ID	BESCHREIBUNG	PRODUKTE
Kennwortwarnungen	100033	Kennwort kann nicht zurückgesetzt werden	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100432	Das Kennwort kann nicht geändert werden. Das neue Kennwort muss sich vom aktuellen Kennwort unterscheiden.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100439	Das Kennwort kann nicht geändert werden. Die Kennwörter stimmen nicht überein.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100441	Das Kennwort kann nicht geändert werden. Das Kennwortfeld muss ausgefüllt werden.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100442	Das Kennwort kann nicht geändert werden. Das Kennwort erfüllt nicht die von PolicyServer definierten Mindestanforderungen für die Länge.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100443	Das Kennwort kann nicht geändert werden. Ziffern sind nicht zulässig.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer

KATEGORIE	NACHRICHTEN-ID	BESCHREIBUNG	PRODUKTE
Kennwortwarnungen	100444	Das Kennwort kann nicht geändert werden. Buchstaben sind nicht zulässig.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100445	Das Kennwort kann nicht geändert werden. Sonderzeichen sind nicht zulässig.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100446	Das Kennwort kann nicht geändert werden. Das Kennwort darf den Benutzernamen nicht enthalten.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100447	Das Kennwort kann nicht geändert werden. Das Kennwort enthält nicht genügend Sonderzeichen.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100448	Das Kennwort kann nicht geändert werden. Das Kennwort enthält nicht genügend Ziffern.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100449	Das Kennwort kann nicht geändert werden. Das Kennwort enthält nicht genügend Zeichen.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer

KATEGORIE	NACHRICHTEN-ID	BESCHREIBUNG	PRODUKTE
Kennwortwarnungen	100450	Das Kennwort kann nicht geändert werden. Das Kennwort enthält zu viele aufeinanderfolgende Zeichen.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100451	Das Kennwort kann nicht geändert werden. Das neue Kennwort muss sich von allen zuvor verwendeten Kennwörtern unterscheiden.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	100452	Ändern des Kennworts fehlgeschlagen - Interner Fehler	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	101003	Festes Kennwort wurde geändert.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Kennwortwarnungen	700100	Kennwort auf festes Kennwort zurückgesetzt.	FileArmor SP6 oder früher
Kennwortwarnungen	700101	Kennwort auf Smartcard zurückgesetzt.	FileArmor SP6 oder früher
Kennwortwarnungen	700102	Kennwort auf Domänenauthentifizierung zurückgesetzt.	FileArmor SP6 oder früher

KATEGORIE	NACHRICHTEN-ID	BESCHREIBUNG	PRODUKTE
Kennwortwarnungen	900159	Das Kennwort kann nicht geändert werden.	KeyArmor
Kennwortwarnungen	900160	Das Kennwort wurde erfolgreich geändert.	KeyArmor
Kennwortwarnungen	900302	Kennwort auf festes Kennwort zurückgesetzt.	KeyArmor
Kennwortwarnungen	900303	Kennwort auf Smartcard zurückgesetzt.	KeyArmor
Kennwortwarnungen	900304	Kennwort auf Domänenauthentifizierung zurückgesetzt.	KeyArmor
PIN-Änderungswarnungen	100438	PIN kann nicht geändert werden. Die PINs stimmen nicht überein.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
PIN-Änderungswarnungen	100440	PIN kann nicht geändert werden. Eines der Felder ist leer.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
PIN-Änderungswarnungen	100453	PIN kann nicht geändert werden. Die PINs stimmen nicht überein.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer

KATEGORIE	NACHRICHTEN-ID	BESCHREIBUNG	PRODUKTE
PIN-Änderungswarnungen	100454	Änderung der PIN möglich. Die neue PIN muss sich von der alten PIN unterscheiden.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
PIN-Änderungswarnungen	100455	PIN kann nicht geändert werden. Die neue PIN erfüllt nicht die von PolicyServer definierten Mindestanforderungen für die Länge.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
PIN-Änderungswarnungen	100456	PIN kann nicht geändert werden. Die PIN darf den Benutzernamen nicht enthalten.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
PIN-Änderungswarnungen	100457	PIN kann nicht geändert werden. Die neue PIN muss sich von allen zuvor verwendeten PINs unterscheiden.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
PIN-Änderungswarnungen	100458	Ändern der PIN fehlgeschlagen - Interner Fehler	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Smartcard-Warnungen	104002	Registrierte Smartcard.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer

Kategorie	Nachrichten-ID	Beschreibung	Produkte
Smartcard-Warnungen	104004	Smartcard kann nicht registriert werden. Prüfen Sie, ob die Karte ordnungsgemäß eingelegt wurde und die Smartcard-PIN gültig ist.	Full Disk Encryption, FileArmor, DriveArmor, KeyArmor oder PolicyServer
Windows Mobile Warnungen	800000	OTA-Installation gestartet	Full Disk Encryption für Windows Mobile
Windows Mobile Warnungen	800001	OTA-Installation abgeschlossen	Full Disk Encryption für Windows Mobile
Windows Mobile Warnungen	800100	OTA-SMS-Nachricht gesendet	Full Disk Encryption für Windows Mobile
Windows Mobile Warnungen	800200	OTA-Verzeichnisliste empfangen	Full Disk Encryption für Windows Mobile
Windows Mobile Warnungen	800300	OTA-Geräteattribute empfangen	Full Disk Encryption für Windows Mobile
Windows Mobile Warnungen	800400	OTA-Gerätesicherung	Full Disk Encryption für Windows Mobile
Windows Mobile Warnungen	800500	OTA-Gerätewiederherstellung	Full Disk Encryption für Windows Mobile



Stichwortverzeichnis

A

Active Directory, 1-17, 1-21, 4-24
Kennwort zurücksetzen, 4-27
Authentifizierung, 1-9
Anwendungsvergleich, 1-14
ColorCode, 1-16, 1-18, 5-6, 6-5
ColorCode erstellen, 5-7
Domäne, 1-17
Domänenauthentifizierung, 1-16
Erstmals, 6-2
Festes Kennwort, 1-16, 1-17, 7-3
FileArmor, 6-2
Full Disk Encryption Preboot, 5-2
Info über, 1-13
Kennwort ändern, 6-6
KeyArmor, 7-2
zum ersten Mal, 7-2
Kontentypen, 1-13
LDAP, 1-17
Methode ändern, 5-5, 5-7
Methoden, 1-16
Optionen, 1-15
PIN, 1-16, 1-18, 6-5
Remote-Hilfe, 1-16, 1-19, 5-9, 5-10
Selbsthilfe, 1-16, 1-19, 4-27, 5-13
Antworten, 5-14
verwenden, 5-14
Setup-Voraussetzungen, 1-17
Sicherheitsoptionen, 1-15
Single-Sign-On, 6-3
Smartcard, 1-19, 5-11, 6-4
Voraussetzungen, 1-17
Zugriffssteuerung, 1-14

B

Begriffe, xii–xiv
Benutzer, 4-1, 4-10
Active Directory-Kennwörter, 4-27
AD-Benutzer importieren, 4-13
ändern, 4-15
Aus Gruppe entfernen, 4-22
Externer Verzeichnis-Browser, 4-13
Gruppenmitgliedschaft, 4-15
Gruppen- und Unternehmensänderungen, 4-15
hinzufügen, 4-10
In eine Gruppe installieren, 4-21
Kennwörter, 4-24
Mit CSV importieren, 4-12
Neuen Benutzer zur Gruppe hinzufügen, 2-8, 4-16
Neuen Unternehmensbenutzer hinzufügen, 2-10, 4-10
Standardgruppe ändern, 4-20
Suchen, 4-14
Vorhandenen Benutzer zur Gruppe hinzufügen, 2-12, 4-18
Benutzer importieren, 4-12, 4-13
Benutzer und Gruppen, 2-6
Benutzer verwalten, 2-5
Berichte, 1-2, 1-9, 8-1, 8-6
Alarm, 8-9, 8-10
Anzeigen von Berichten, 8-10
Fehler anzeigen, 8-11
Optionen, 8-6
Standard, 8-8, 8-9
Symbole, 8-7
Typen, 8-7

Zeitgesteuerte Berichte, 8-11
Bildschirmtastatur, 5-4
Bootsektor wiederherstellen, 5-21

C

Client-Server-Architektur, 1-2
ColorCode, 1-18, 5-6
Command Line Helper, 5-2
Command Line Helper Installationsprogramm, 5-2
Community, 9-2
csv, 4-12

D

DAAutoLogin, 5-2
Datenbankanforderungen, 1-5
Datenschutz, 1-2
Datenwiederherstellung, 5-31
Demilitarisierte Zone, 5-15
Discs brennen, 6-16
Domänenauthentifizierung, 1-17
FileArmor, 6-3

E

Endpunktverschlüsselung
Info über, 1-2
Tools, 5-2
Entschlüsselung
Wiederherstellungskonsole, 5-19

F

Fehlermeldungen
Authentifizierung, 1-15
Festes Kennwort, 1-17
Festplatte entschlüsseln, 5-19
FileArmor, 6-1
archivieren, 6-11
Archivieren und brennen, 6-11, 6-16
Archiv mit festen Kennwort brennen, 6-16
Archiv mit Zertifikat brennen, 6-16
Authentifizierung, 6-2
Domäne, 6-3
Optionen, 1-15
PIN, 6-5
ColorCode, 6-5
Dateiverschlüsselung, 1-10
digitales Zertifikat, 6-15
erstellen, 6-15
Erste Verwendung, 6-2
fester Kennwortschlüssel
erstellen, 6-14
Gemeinsamer Schlüssel, 6-13
erstellen, 6-13
Gerät entsperren, 6-7
Kennwort ändern, 6-6
Kennwort zurücksetzen, 6-6, 6-8
lokaler Schlüssel, 6-12
Mit PolicyServer synchronisieren, 6-10
Offline-Dateien synchronisieren, 6-10
PolicyServer Synchronisierung, 6-8
PolicyServer wechseln, 6-11
Remote-Hilfe, 6-7, 6-8
Sicheres Löschen, 6-17
Single-Sign-On, 6-3
Smartcards, 6-4, 6-5
Symbol in der Task-Leiste, 6-8
Systemvoraussetzungen, 1-7
Task-Leistensymbol
Info über, 6-8
Unterstützte Betriebssysteme, 1-7
Verschlüsselung, 6-11
Zeitverzögerung, 6-8
Zugriffssteuerung, 1-14

FIPS, 1-2
FIPS 140-2, 1-2, 1-11
Info über, 1-11
KeyArmor, 7-12
Sicherheitsstufen, 1-11
FIPS 140-2, 1-2
Full Disk Encryption, 5-1
3.1.3 Verbesserungen, 1-22
Authentifizierung, 1-19, 5-13
Kennwort ändern, 5-6
Optionen, 1-15
Benutzer verwalten, 5-22
Dateien entfernen, 5-32
Deinstallieren, 5-27
Festplatte entschlüsseln, 5-19
Gerät entfernen, 4-35
Konnektivität, 5-15
Menüoptionen, 5-3
Netzwerkkonfiguration, 5-25
Netzwerk-Setup, 5-25
Nicht verwaltete Installation
Benutzer, 5-22
PolicyServer Einstellungen, 5-15
PolicyServer wechseln, 5-26
Porteinstellungen, 5-15
Remote-Hilfe, 5-10
Richtlinien verwalten, 5-24
Selbsthilfe, 5-13
smartcards, 1-19, 5-11
Synchronisierung von Richtlinien, 5-16
Systemvoraussetzungen, 1-6
TCP/IP-Zugriff, 5-15
Tools, 5-2
Unternehmen wechseln, 5-26
Unterstützte Betriebssysteme, 1-6
Wiederherstellungskonsole, 5-18
Windows, 5-18
Wiederherstellungsmethoden, 5-27
Zugriffssteuerung, 1-14
Full Disk Encryption Preboot, 5-2
Authentifizierung, 5-5
Bildschirmtastatur, 5-4
Menüoptionen, 5-3
Netzwerkverbindung, 5-4
Tastaturbelegung, 5-5

G

Geräte, 4-1, 4-32
Attribute anzeigen, 4-36
Aus Gruppe entfernen, 4-34
Befehl "Auslöschen", 4-38
Neu starten, 4-39
Sperren, 4-38
Verzeichnis anzeigen, 4-36
Verzeichnisüberwachung, 4-37
Zur Gruppe hinzufügen, 4-32
Geräteverwaltung, 1-9
Gruppen, 4-1
ändern, 4-5
entfernen, 4-5
Gerät entfernen, 4-34, 4-35
In eine Gruppe installieren, 4-21
Offline-Gruppen, 4-5
Offline-Gruppen erstellen, 4-6
Typen, 4-2
Untergruppen, 4-2
Gruppen verwalten, 2-5

H

Hardware-basierte Verschlüsselung, 1-6
Helpdesk-Richtlinien, 4-31

I

Info über

Benutzer und Gruppen, 2-5
Client-Server-Architektur, 1-2
Endpunktverschlüsselung, 1-2
FileArmor, 6-1
KeyArmor, 7-1
Kontentypen, 1-13
PolicyServer, 2-1, 2-2

K

Kennwort
Selbsthilfe, 4-27
Kennwörter, 1-12, 4-24
Active Directory-Kennwort zurücksetzen, 4-27
Auf ein festes Kennwort zurücksetzen, 4-26
Benutzerkennwort zurücksetzen, 4-26
Für Administrator/Authentifzierer zurücksetzen, 4-24
Für Gruppenadministrator/ Authentifzierer zurücksetzen, 4-25
Kennwort für Unternehmensauthentifizierer zurücksetzen, 4-24
Remote-Hilfe, 4-29
Zurücksetzen, 4-25
Kennwörter ändern, 5-6
KeyArmor, 7-1
Abmelden, 7-7, 7-8
Aktivitätsprotokollierung, 7-14
Antivirus-Updates, 7-5
Authentifizierung, 7-2
Festes Kennwort, 7-3
Methoden, 7-3
Optionen, 1-15
zum ersten Mal, 7-2
Dateien schützen, 7-13
Festplattenüberprüfung, 7-6
FIPS, 7-12
gelöschtes Gerät, 7-18
Gerätekomponenten, 7-4
hilfe
Selbsthilfe, 7-11
Hilfe
Falls gefunden, 7-8
Remote-Kennwortzurücksetzung, 7-11
Support-Informationen, 7-12
Hilfe (Menü), 7-8
Info über, 7-7, 7-8
keine Informationen hinterlassen, 7-5
Kennwort ändern, 7-7, 7-8
menü, 7-8
neu zuweisen, 7-17
PolicyServer, 7-14
Richtlinien-Updates, 7-7, 7-8
Schlüsselverwaltung, 1-11
Sichere Daten, 7-7, 7-8
sicher entfernen, 7-6, 7-14
SICHERES LAUFWERK, 7-4
Systemvoraussetzungen, 1-8
Taskleiste, 7-7, 7-8
Temporär, 7-6
Unverschlüsselte Geräte, 7-6
Verschlüsselung, 7-5
verwenden, 7-6
Virenschutz, 7-15
Update-Speicherort ändern, 7-15
Vollständige Suche, 7-15
Warnung, 7-6
Zugriffssteuerung, 1-14
Zwischengespeicherte Dateien, 7-6
Konten

Typen, 1-13
Kryptographie, 1-2

L
LDAP, 1-17
LDAP-Proxy, 1-21, 4-10

M
MBR
Ersetzen, 5-21

N
Netzwerk-Setup, 5-25

O
Online
Community, 9-2
OPAL, 1-6

P
Partitionen bereitstellen, 5-21
Persönliche Identifikationsnummer (PIN), 1-18
PolicyServer
3.1.3 Verbesserungen, 1-21
ändern, 5-26
Anwendungen aktivieren, 2-18
Authentifizierung, 2-2
Optionen, 1-15
Benutzer, 2-5, 4-10
Unternehmensbenutzer hinzufügen, 2-8, 4-16
Zur Gruppe hinzufügen, 2-8, 2-12, 4-16, 4-18
Benutzeroberfläche, 2-3
Benutzer und Gruppen, 2-6
Berichte, 8-1, 8-6
Client-Web-Service, 1-2
Einführung, 2-2
Erste Schritte, 2-1
Erstverwendung, 2-2
Erweiterter Standort, 8-5
Felder und Schaltflächen, 2-15
Geräte, 4-32
Gruppen, 2-5
Benutzer hinzufügen, 2-8, 4-16
Lizenzdatei, 2-2
MMC-Fenster, 3-2
MMC-Hierarchie, 2-4
Offline-Gruppen, 4-5
Aktualisieren, 4-9
erstellen, 4-6
Protokolle, 8-1
Protokollereignisse, 8-2
Protokollwarnungen einrichten, 8-3
Remote-Hilfe, 4-29
Richtlinien, 2-14, 3-1, 3-2
Allgemein, 3-47
Bearbeiten, 3-3
Mehrere Optionen, 3-11
Mehrfachauswahl, 3-7
Richtlinien mit Bereichen, 3-3
Textzeichenfolge, 3-10
Wahr/Falsch, Ja/Nein, 3-5
DriveArmor, 3-41
FileArmor, 3-27
Full Disk Encryption, 3-19
KeyArmor, 3-37
MobileSentinel, 3-32
PolicyServer Richtlinien, 3-13
Support-Informationen, 4-31
Richtlinien ändern, 2-16
SMS/E-Mail-Versand weiterleiten, 8-4
Software-Voraussetzungen, 1-5

Support-Informationen, 4-31
Systemvoraussetzungen
hardware, 1-5
Top-Gruppe hinzufügen, 2-6, 4-2
Untergruppen, 4-4
Unternehmensbenutzer hinzufügen, 2-10, 4-10
Verbesserungen, 1-20
Voraussetzungen
SQL, 1-5
Voraussetzungen für SQL, 1-5
Web-Service, 1-2
Zugriffssteuerung, 1-14
PolicyServer MMC, 1-2
PolicyServer wechseln, 5-26
Produktdefinitionen, xii–xiv
Produktkomponenten, 1-2
Protokolle, 5-25, 8-1
Ereignisse verwalten, 8-2
Warnungen, 8-3
Warnungen einrichten, 8-3
Protokollereignisse, 8-2

R

Remote-Hilfe, 1-19, 4-24, 4-29, 4-38, 5-9
Reparatur-CD, 5-2, 5-27, 5-29
Datenwiederherstellung, 5-31
Entschlüsselung, 5-31
Richtlinien, 1-12
Allgemein, 3-47
Agent, 3-47
Authentifizierung, 3-47
DriveArmor, 3-41
Authentifizierung, 3-42
Gerät, 3-46
Kommunikation, 3-44
FileArmor
Computer, 3-27
Kennwort, 3-31
Verschlüsselung, 3-27
Full Disk Encryption, 3-19
Allgemein, 3-19
PC, 3-21
PPC, 3-25
KeyArmor, 3-37
Anmelden, 3-38
Hinweismeldung, 3-40
PolicyServer Verbindung, 3-41
Sicherheit, 3-38
Virenschutz, 3-37
MobileSentinel, 3-32
Allgemein, 3-32
PPC, 3-34
PolicyServer, 3-13
Administrator, 3-14
Admin-Konsole, 3-13
Authentifizierer, 3-15, 3-16
Begrüßungsnachricht, 3-18
Herunterladen von Service Packs, 3-18
PDA, 3-16
Protokollwarnungen, 3-16
Support-Informationen, 4-31
Synchronisierung, 1-10
Synchronisierung von Clients, 5-16
Wiederherstellung durch Benutzer zulassen, 5-18
Richtliniensteuerung, 1-10, 6-1

S

Schlüsselverwaltung, 1-11
Seagate DriveTrust-Laufwerke, 1-6
Selbsthilfe, 1-19, 4-24, 5-13
Antworten, 5-14

Antworten festlegen, 5-13
Kennwortunterstützung, 4-27
Sicherheit
Antivirus-/Anti-Malware-Schutz, 1-2
Gerätesperre, 1-19, 5-9
Gerät löschen, 1-15
Kontosperraktion, 1-19, 5-9
Kontosperre, 1-19, 5-9
Remote-Authentifizierung erforderlich, 1-15
Zeitraum bis Kontosperrung, 1-19, 5-9
Zeitverzögerung, 1-15
Zulässige Anzahl fehlgeschlagener Anmeldeversuche, 1-19, 5-9
Smartcard, 1-19, 5-11
software, 1-5
Support
Knowledge Base, 9-2
Schnellere Problemlösung, 9-3
TrendLabs, 9-4
Symbol in der Task-Leiste, 6-8
Synchronisierung
FileArmor, 6-10
Synchronisierung von Richtlinien, 5-16
Systemarchitektur, 1-2
Systemvoraussetzungen
FileArmor, 1-7
Full Disk Encryption, 1-6
KeyArmor, 1-8
PolicyServer, 1-5

T

Token, 5-12
Tools
Reparatur-CD, 5-29
Top-Gruppe, 2-6, 4-2
TrendLabs, 9-4

U

Überlegungen zu Windows Server 2008, 1-5
Unterstützte Sprachen, 1-20

V

Verschlüsselung, 1-10, 3-27
Archivieren, 6-16
Datei und Ordner, 1-10
Dateiverschlüsselung, 6-1
digitales Zertifikat, 6-15
fester Kennwortschlüssel, 6-14
FileArmor
Archivieren und brennen, 6-11
FIPS, 1-11, 7-12
Funktionen, 1-9
Hardware-basiert, 1-10
KeyArmor, 7-5
lokaler Schlüssel, 6-12
Schlüssel
gemeinsame, 6-13
selbstextrahierend, 6-14
Software-basiert, 1-10
Vollständige Festplatte, 1-10
verstehen
Dateiverschlüsselung, 1-10
Endpunktverschlüsselung, 1-1
FIPS, 1-11
full disk encryption, 1-10
Schlüsselverwaltung, 1-11
VMware Virtual Infrastructure, 1-5

W

Warnungen, 8-3
Wichtigste Funktionen, 1-9
Wiederherstellung
Dateien entfernen, 5-32
Wiederherstellungskonsole, 5-16

Anmelden, 5-18
Benutzer
Bearbeiten, 5-23
Hinzufügen, 5-23
Löschen, 5-24
Benutzer verwalten, 5-22
Bootsektor wiederherstellen, 5-21
Festplatte entschlüsseln, 5-19
Funktionen, 5-16
Netzwerkkonfiguration, 5-25
Netzwerk-Setup, 5-25
Partitionen bereitstellen, 5-21
Protokolle anzeigen, 5-25
Reparatur-CD, 5-31
Richtlinien verwalten, 5-24
Unternehmen oder Server wechseln, 5-26
Wiederherstellungsmethoden, 5-27
Zugreifen, 5-18
Windows, 5-18
Wiederherstellungsmethoden, 5-27
Windows 8, 1-6

Z

Zentrale Verwaltung, 1-9, 1-12
Zugänglichkeit
Bildschirmtastatur, 5-4



TREND MICRO INCORPORATED
10101 North De Anza Blvd. Cupertino, CA., 95014, USA
Tel:+1(408)257-1500/1-800 228-5651 Fax:+1(408)257-2003 info@trendmicro.com

www.trendmicro.com

Item Code: APGM35732/121016